2004 Command and Control Research and Technology Symposium

The Power of Information Age Concepts and Technologies

CHALLENGES FOR VERTICAL COLLABORATION AMONG WARFIGHTERS FOR MISSILE DEFENSE C2

Laura A.T. Lee
Director, C2 Systems
laura.lee@sparta.com

Ray C. Prouty
Chief Engineer
ray@sparta.com

David J. Sepucha
Sr. Software Developer
david_sepucha@sparta.com

SPARTA, Inc.
13400 Sabre Springs Parkway, Suite 220
San Diego, California 92128

Telephone: (858) 668-3570, FAX (858) 668-3575

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Challenges for Vertical Collaboration Among Warfighters for Missile Defense C2	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Sparta Inc,13400 Sabre Springs Parkway Suite 220,San Diego,CA,92128**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**51**	

CHALLENGES FOR VERTICAL COLLABORATION AMONG WARFIGHTERS FOR MISSILE DEFENSE C2

Abstract

Implementing an effective Missile Defense plan in a Network Centric environment requires a robust collaboration scheme – compatible with multiple military models and simulations. Many technology breakthroughs have occurred allowing defense plans to be rapidly exchanged with C2 systems distributed around the Globe. However, the issue of *interpreting* the data properly within each C2 model or simulation component remains a stumbling block to effective planning. This paper describes a global collaboration approach using the eXtensible Mark-up Language (XML) to create and validate the plans. Experimentation performed using this approach, by allowing plans to be distributed using a Java Message Service (JMS) or provided by web services, is described to highlight the issues with netted sensors and weapons in military planning. An approach to resolving this issue through a higher level NCW model of the architecture supported by tactical element web services is shown.

1.0 Introduction

The revolution in information technology offers many promises for enabling Network Centric Warfare (NCW). To reach this potential, however, we cannot just apply the new technology to existing weapon and sensor systems. Collaboration in Missile Defense planning is a good example of the challenges of applying the new concepts and technologies to systems designed before the birth of NCW. The missile defense architecture has been in concept development and design for almost twenty years – how can we reap the benefits of NCW without starting over in the element design? In this paper, we begin to identify options for creating net-centric capabilities in missile defense.

1.1 Caveat

For clarification, this work is the authors' own ideas and concepts and does not represent the view of the Missile Defense Agency (MDA) in any official manner. This detachment offers an opportunity to explore ideas that might not otherwise be exchanged to stimulate interest in several related fields.

1.2 Missile Defense Planning Overview

The systems about to be deployed in 2004 by the Missile Defense Agency (MDA) to protect the U.S. and our allies have their roots in legacy Army, Navy, Air Force and Marine Corps programs. These systems generally consist of a sensor, one or more weapons and their associated command, control, battle management, and communications (C2BMC) for the element. Each system element created a planner in order to assist warfighters in the employment of that system. Multiple systems were designed to be deployed in a defense architecture with the planners focusing on the deconfliction of fires to reduce wastage among different systems. The planning of the defense architecture is in response to high level guidance, but generally has been performed at the lowest tactical level where the complexities of the system are best understood. Prior to 2004, this planning could be accomplished within a single Army workstation. Multiple workstations have been deployed across the globe within the Army military structure and the collaboration among these units – horizontally – was envisioned to create the defense shield.

This year, the sensors designed by each of the military services are being deployed in a network with various weapon systems. Sensor data from one previously stove-piped system may now provide critical tracking data to be used by a weapon system developed by another program in another branch of the military. To develop an accurate assessment of defense capabilities as input to the selection of a friendly Course of Action (COA), the missile defense plans must be able to consider this cross-system, cross-service – ***net-centric*** – operation.

1.3 Scope and Organization of Paper

In this paper, we introduce *requirements* for missile defense planning in order to operate in a Net-Centric environment across the globe and across different warfighting areas of responsibility (AORs). In section 2, we explain a simple defense planning analysis and gradually add the complexities to the situation to illustrate basic missile defense planning concepts. In section 3, we focus on the vertical coordination challenges along with the traditional horizontal (cross-AOR) coordination. In section 4, we discuss the

technologies and approaches used for collaboration to include a description of the key enterprise services envisioned in the Global Information Grid (GIG). In section 5, we describe multiple concepts for collaborating on missile defense plans. These concepts range from the monolithic, large scale, (broad and detailed) planning tool to distributed sensor and weapon planning web services. In section 6, we conclude with a summary of the recommended next steps in planning for net-centric operations.

2.0 Developing a Missile Defense Plan

In the near term, MDA is beginning deployment of a Missile Defense architecture comprised of the Army's PATRIOT sensors and weapons, the Navy's AEGIS destroyer and cruise class ships with a sensor, the Army's Ground-Based Radar (experimental), the Army's Ground-Based Interceptors (GBI), Upgraded Early Warning Radars (UEWR), the Cobra Dane Radar and the Air Force's experimental Air-Borne Laser (ABL). This architecture is depicted in Figure 2-1.

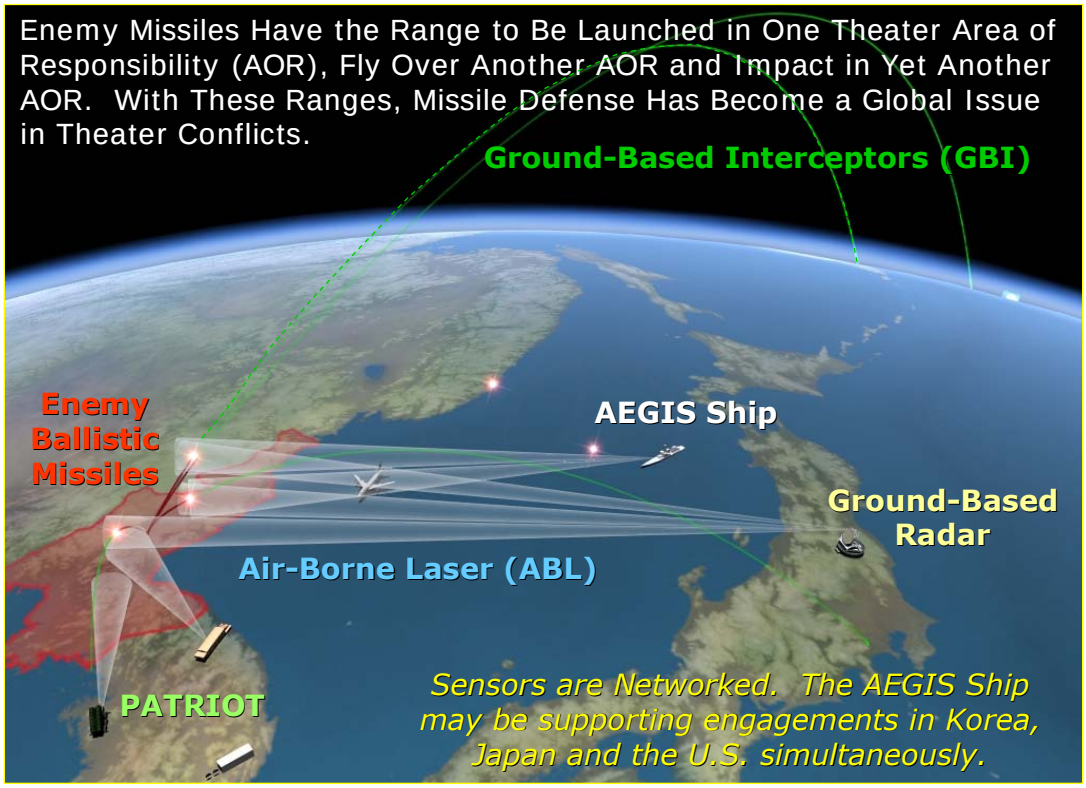


Figure 2-1: Basic Missile Defense Architecture

In this example, an enemy missile is launched in one AOR, flies over another AOR and impacts in yet a third AOR, if not successfully intercepted. With networked sensors, the AEGIS ship can be used to support engagements in Korea, Japan and the U.S. simultaneously. A similar multi-AOR capability is possible for the ABL.

The complete missile defense plan must consider these complex sensors – distributed around the world. The plan typically includes ten's of defense systems, some engaged in *multiple* missions and deployed to support different commanders (in *multiple* AORs) to intercept *multiple* threat types. To develop this plan, the individual systems have detailed planners or are in the process of developing them for their defense system. However, each of these planners considers only its own sensor - not net-centric operation. What role could these planners have in developing an integrated plan for an NCW architecture?

Walking through the details of plan development may shed some light. In Figure 2-2, the initial guidance for planning is shown. In red is an example ballistic missile launch site with a range ring for its minimum capability. The maximum range of the enemy missile is beyond the map view. In green, four different possible friendly assets are displayed. These assets could be airports, seaports or population centers, for example. Looking at the potential launches from the enemy sites to each of the friendly assets is the next step in planning.

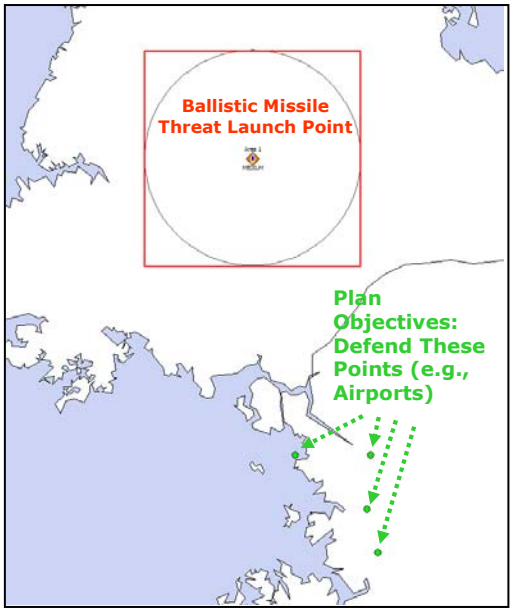


Figure 2-2: Planning Begins with Enemy Launch Points and Friendly Assets to be Protected

In Figure 2-3, two analytical cases are shown. On the left, each potential trajectory from the estimated launch site is drawn. The probability of negation (Pn) for the defense system against each trajectory is outlined (the value of Pn determines the color). On the

right side of Figure 2-3, a potential Enemy Course of Action (ECOA) is shown. The ECOA is an example of a likely enemy action to include the number of missiles launched, launch timing and tactics. A basic plan first evaluates the feasibility of engaging all likely missile trajectories to determine defense deployment and architecture composition. The plan must then be evaluated against several ECOAs to understand vulnerabilities to raid size and sustainability of defense given available inventory.

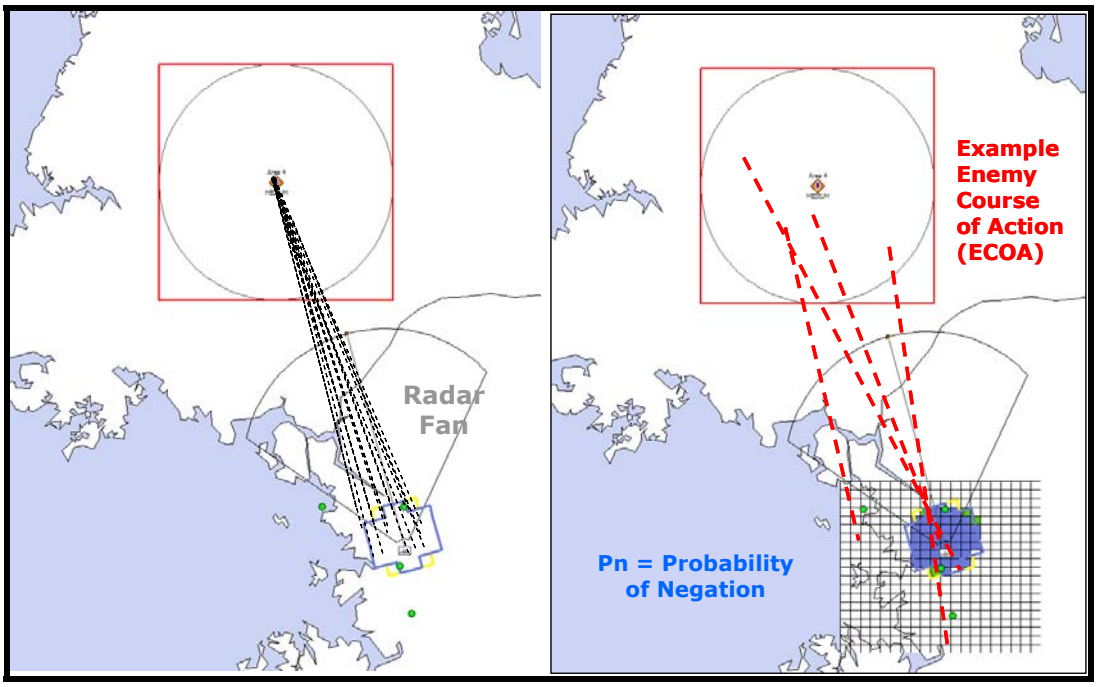


Figure 2-3: Calculating Defense Probability of Negation

In the early development of the missile defense systems, each system designed a detailed tactical planner to assist in the deployment and use of that weapon system. Mission guidance flowed down from the strategic and operational level to the tactical level where the detailed planning occurred. The operational level would determine the particular mission or assets for PATRIOT to protect or for THAAD to protect or for AEGIS BMD to protect. Each planning system would evaluate the enemy threats and assigned assets to determine their optimal basing and capability. The various tactical plans would be transmitted up from the tactical to the operational level, as shown in Figure 2-4. With these stove-type systems then, the missile defense plan could be developed from the bottoms up – starting with top-level mission guidance.

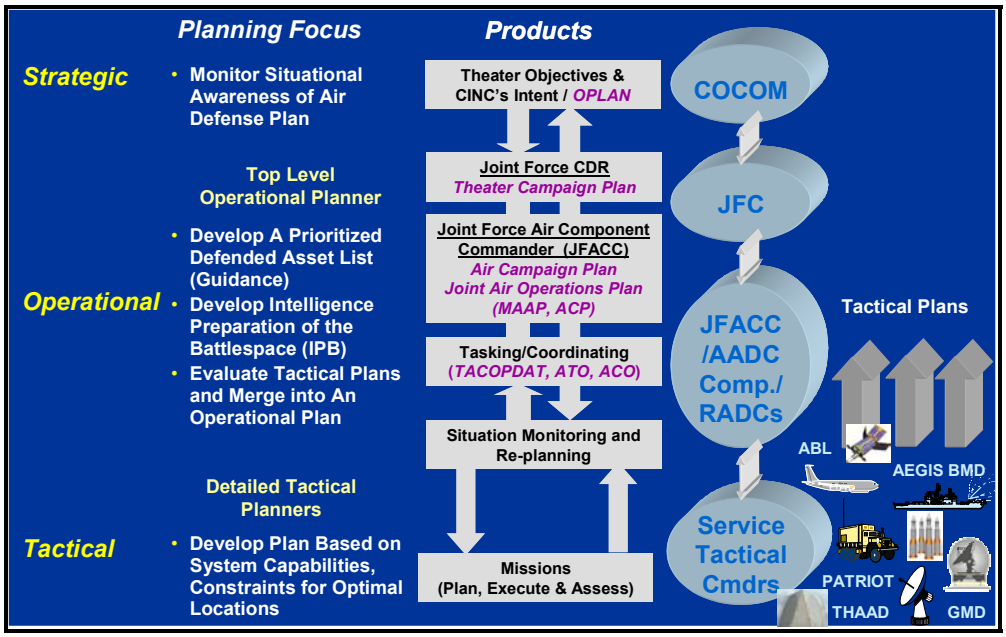


Figure 2-4: Developing a Plan (Pre-Network Centric Warfare)

Figure 2-5 shows a cartoon of the "integration" of a plan that is really the loose sum of the individual system plans put together. Each system roughly fits together in the plan, protecting its own assets. Coordination of firing strategy, however, needs to occur if the different defense systems have overlapping capabilities or there will be missile wastage.

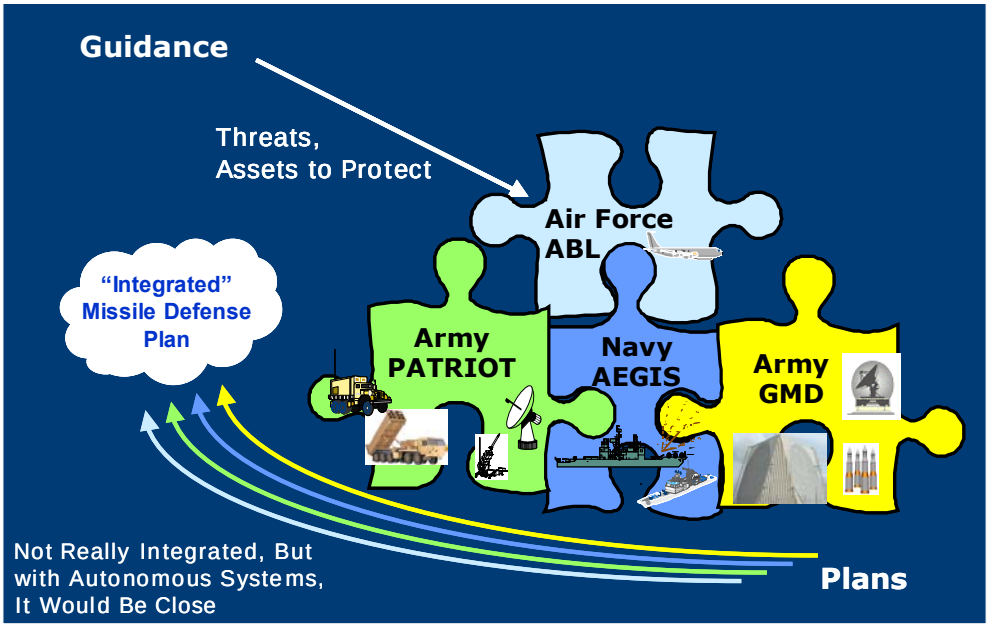


Figure 2-5: Building the Approximate Operational Plan

Missile Defense planning for the architecture is much more complicated than the previous example (Figure 2-3) illustrates for a single threat - single defense. In the real world, multiple threat types and locations must be evaluated against multiple defense systems – some performing multiple missions. In addition, these multiple systems interact, such as providing radar cueing or threat tracking data for the interceptors in a sensor network. Finally, these systems may belong to different chains of command (e.g., different AORs). The integrated missile defense plan must be able to handle all of these complexities while handling the interactions inherent in NCW operations. Figure 2-6 illustrates the increasing complexity of missile defense planning, showing the simple example as the starting point. Even in the simplest examples, the defense protection varies in probability of negation due to threat azimuth, range, velocity and impacts of terrain.

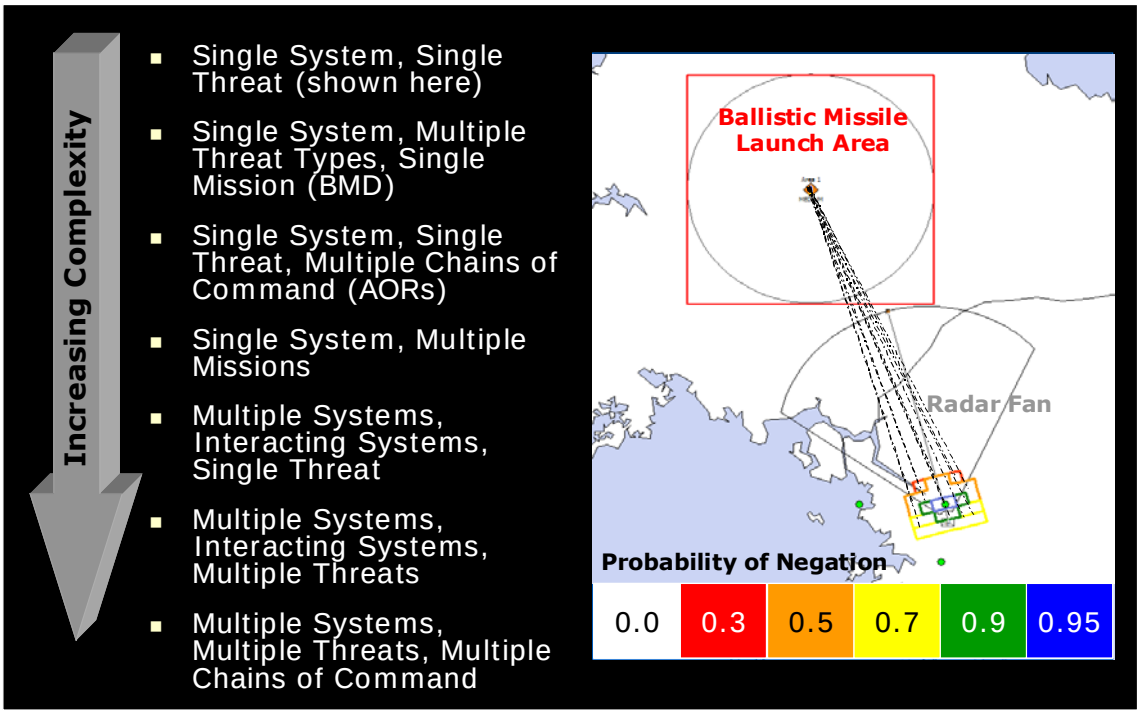


Figure 2-6: Increasing Complexity of Missile Defense Plans

In Figure 2-7, we show a notional, real-world architecture. There are many different possible threat locations - some shown as points, others as polygons. Many PATRIOT

systems are arrayed near the critical assets and other longer range radars based at sea or on land can be seen.

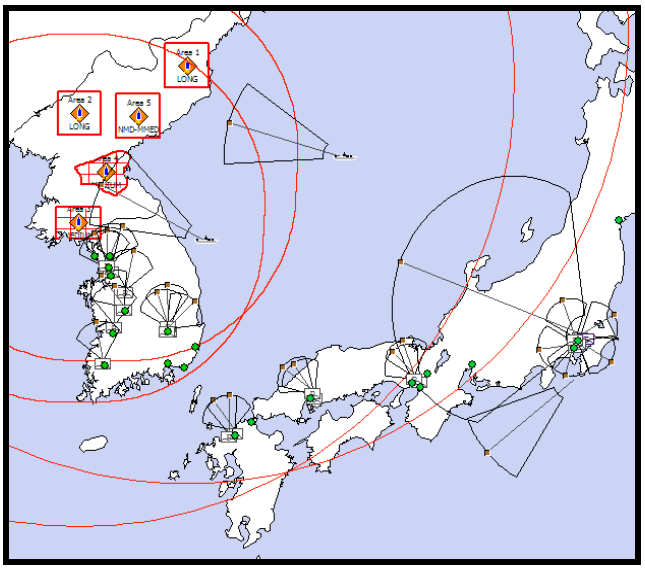


Figure 2-7: Example Complex Architecture

This complexity is further illustrated in Figure 2-8, where the depth of water and terrain is viewable. In this example, the distributed sensors (e.g., AEGIS, GBR) will interact with non-collocated weapon systems (e.g., GBI) to protect several regions of interest (e.g., Korea, Japan and the US).

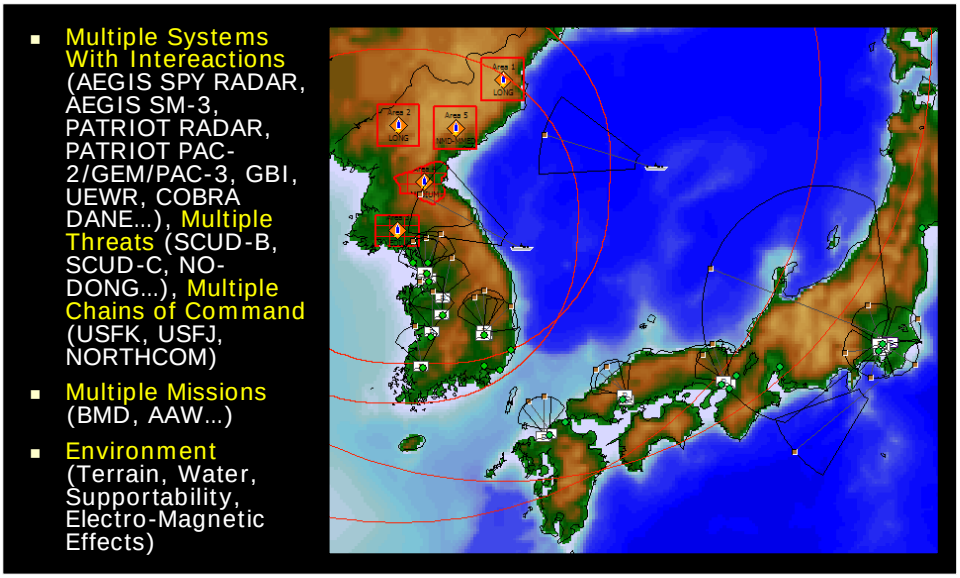


Figure 2-8: Real-World Missile Defense Architecture

3.0 Vertical Coordination Challenges

In the Missile Defense community, plans are developed in each region of the world or AOR and are exchanged *horizontally* among various combatant commanders -- eventually brought together into a single Integrated Missile Defense (IMD) plan by USSTRATCOM. Efforts are underway to extend the horizontal, distributed, collaborative planning *vertically* – allowing the exchange of plans from operational C2 systems to tactical level systems. The spectrum of horizontal and vertical collaboration is illustrated in Figure 3-1. When an operational level plan is transmitted to a tactical system (e.g., AEGIS BMD), the tactical C2 systems can interpret the context of their system within the entire Net-Centric Operation or only use the data relevant to their specific sensor and/or weapon (each approach has unique benefits and challenges). Difficulties occur when the high-fidelity tactical systems try to "optimize" their role in NCW without understanding the full architecture capability and warfighting concepts. Effective vertical collaboration requires both the technologies and concepts for transmitting plans and an NCW framework for interpreting them.

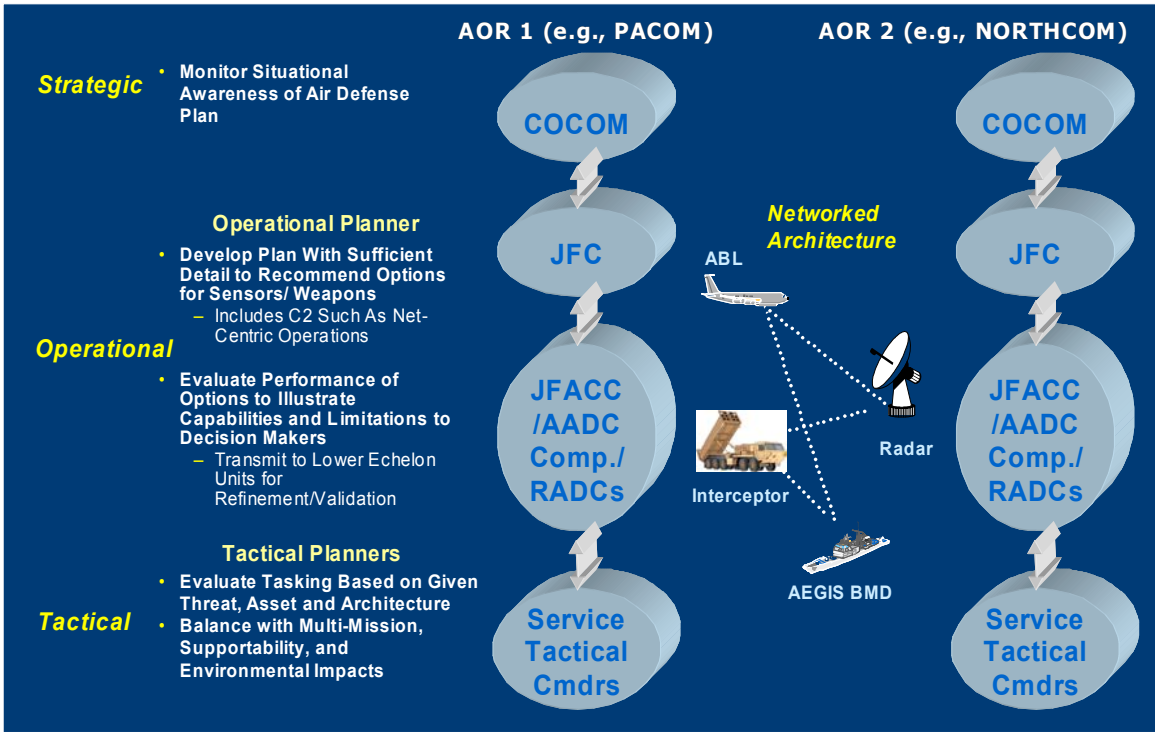


Figure 3-1: Vertical Planning In NCW – Across AORs

One of the key challenges can be illustrated on the cartoon of systems shown in Figure 3-1. The cartoon represents a networked architecture. In this NCW environment, sensor data from one system will be used to form tracks or launch interceptors located far away. A planner resident at the interceptor site that does not know or understand the distributed sensors has no way to develop a plan with NCW concepts. Furthermore, each planning system, even if it could roughly understand the overall architecture context and the other systems, would not have the detail of the other systems to "optimize" their placement. Issues such as AEGIS operation in littoral warfare or stationing to consider the electro-magnetic interference from another radar or multi-mission anti-air warfare are far too detailed for each planner to digest. **In a nutshell, although tactical planners are very detailed – they are only detailed about their own systems and typically know little, if anything, of the NCW context in which they must operate.**

The planning premise, then, shown in Figure 3-1 is that an operational level planner will know enough about all the systems and their Net-Centric capabilities to formulate an initial plan. Overall architecture performance against all the enemy missiles must be evaluated. Since this operational level planner does not consider the detail of the environment or multi-missions, this plan must be sent to tactical planner systems to be evaluated and changed or validated. With multiple tactical planners, this last step is not trivial – how do planners validate tasks that are performed with other systems they know little about?

4.0 Enabling Technologies

Exchanging plans, coordinating horizontally and vertically, developing plans or validating them in a distributed environment – all sound like common events in today's internet savvy world. Many people believe that the challenges of missile defense planning can be accomplished using chat, whiteboard or the virtual rooms of the Defense Collaboration Tool Suite (DCTS) or the similar InfoWorkSpace (IWS).

The Defense Collaboration Tool Suite (DCTS) is a commercial off-the-shelf (COTS) application providing interoperable, synchronous and asynchronous collaboration capability to the Department of Defense's (DoD) agencies, Combatant Commands and military services. These collaboration tools enhance simultaneous, ad hoc crisis and deliberate continuous operational action planning (vertically and horizontally) across operational theaters and other domains that provide operational units and defense organizations simultaneous access to real-time operational, tactical and administrative information.

DCTS offers voice and video conferencing, document and application sharing, instant messaging and whiteboard functionality in support of defense planning. It enables two or more distributed operational users to simultaneously participate in the mission planning process ("collaborative") without the need to be co-located ("distributed"). With DCTS, military forces enjoy the capability to link various command, control, communications, computers and intelligence (C4I) and mission planning systems together on a common network to share data, conduct collaborative planning and collaboratively consult on information and data at various locations around the world.

These technologies do help the human planners coordinate and discuss planning issues, but the true enabling technologies for vertical coordination center on "web services". Figure 4-1 lists many of the web service standards that are proving to be key to the future for mission planning.

From the early days of the internet, Web technologies have been used to provide an interface to distributed services (e.g., HTML forms). The creation of the eXtensible Markup Language (XML) has accelerated this development, and has sparked the emergence of numerous XML-based environments that enable Web services. These environments include distributed application environments such as protocol conventions, security features, mechanisms to ensure reliable delivery and interface description languages - all of which are adapted to the special needs of the Web environment.

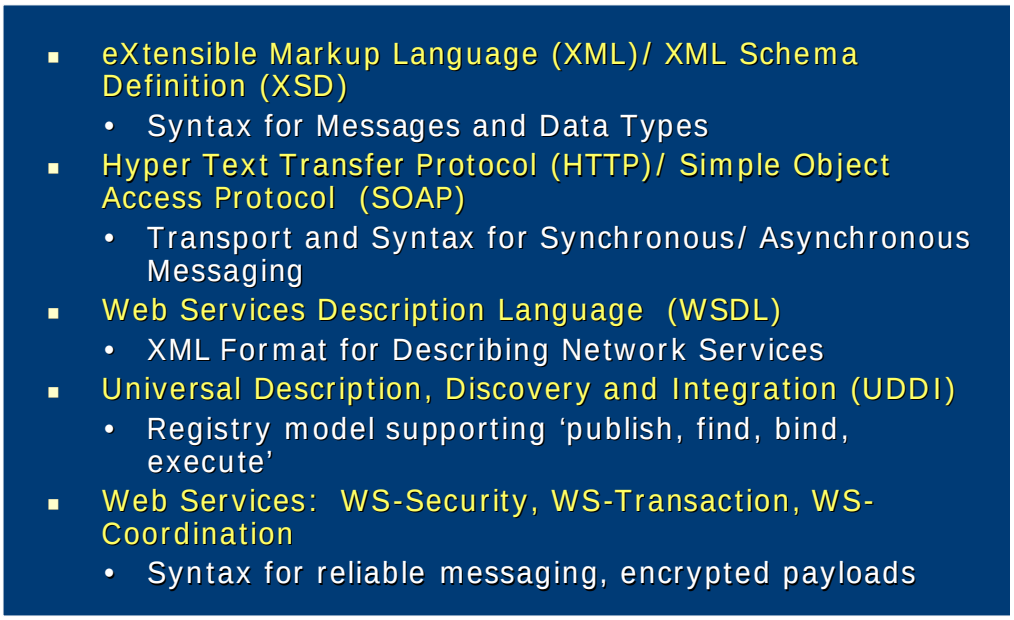


Figure 4-1: Key Standards Supporting Web Services

The term *web services* is fairly self-explanatory; it refers to accessing services over the web. The current use of the term refers to the architecture, standards, technology and business models that make web services possible. IBM published the following definition of web services:

> *Web services are a new breed of Web application. They are self-contained, self-describing, modular applications that can be published, located, and invoked across the Web. Web services perform functions, which can be anything from simple requests to complicated business processes. In other words, web services are interoperable building blocks for constructing applications.*

A standard way of capturing service descriptions is necessary. The web services description language (WSDL) has been developed for this purpose. WSDL describes a service as a set of 'ports' which group related interactions that are possible between the application (service requestor) and the web service (service provider). The interactions that are possible though a port are described as 'operations', which may have an input message and optionally a resulting output message. Each operation describes a potential

interaction with the web service. This may be a request from the application to the web service. It could also be an interaction that can be initiated by the web service for which the application needs to take action. Interactions in either direction can be one-way or can require a response to be sent.

A WSDL describes a service in terms of possible interactions with it; in the case of mission planning, it could be questions that the service can answer. A WSDL document provides the potential information content of interactions with a web service but doesn't explain how to communicate that information between an application and a web service. For this purpose, the WSDL allows a 'binding' to be specified, in practice this is likely to be another XML-based standard, SOAP.

The Simple Object Access Protocol (SOAP) is a standard for XML-based information exchange between distributed applications. Although other transports are possible, SOAP is typically transmitted over HTTP providing a platform for communication with/between web services.

A UDDI web services registry is a web service that can be accessed using SOAP from an application that wishes to discover web services. UDDI specifies interfaces for applications to publish web services (as WSDL documents) and to discover web services (via their WSDL documents). A UDDI entry actually contains more that just a WSDL interface and implementation, it can also include further metadata such as quality of service parameters, payment mechanisms, security and keywords for resource discovery. With these standards we have the infrastructure to publish (WSDL, UDDI), find (WSDL, UDDI) and bind (WSDL, SOAP) web services in an interoperable manner.

Figure 4-2 shows an example of part of an XML schema that we have been developing for missile defense planning. A companion schema is under development for the intelligence parameters for the enemy missiles. These schemas are part of MDA's namespace and are registered with the Defense Information Systems Agency (DISA)

XML registry. Developing these schemas is an important first step in defining the missile defense planning language to allow the exchange of plans.

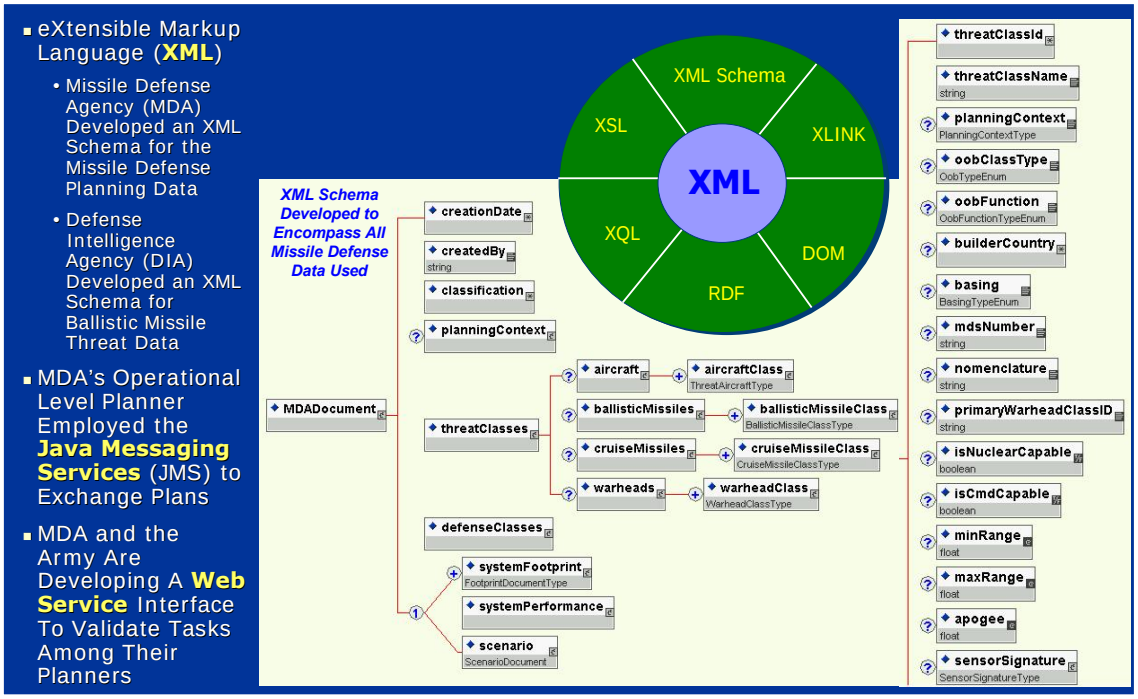


Figure 4-2: Technology Advances Supporting Collaboration Among Planners

With the advent of these web technologies, there are several options available to create the collaboration framework allowing both horizontal and vertical coordination to occur in the development of a missile defense plan for net-centric operations.

5.0 Approaches to Missile Defense Collaboration

Now that we have the requirements for vertical coordination in missile defense planning and the enabling technologies identified, we can turn our attention to different model architecture approaches using those technologies to satisfy the requirements. Although there are many possible solutions, in this paper we consider three basic categories: (1) a large, monolithic simulation; (2) a distributed architecture of federated planners or (3) something we will term a "net-centric planner". The last two approaches may appear to be the same, but the distinguishing feature of the third option (i.e., a net-centric planner) is that there is only one planner or one copy of each function required –distributed and connected via web services.

5.1 Detailed and Broad "One-Sim"

To effectively plan the missile defense architecture that encompasses multiple threat types, multiple defense systems, interacting systems, multiple missions and environmental impacts, a very detailed and broad simulation could be developed. If this simulation, hereafter referred to as "One-Sim", was developed it would be used at both the operational and tactical levels. This concept is illustrated in Figure 5-1.

Figure 5-1: Example of Monolithic "One-Sim" Planner

Although the missile defense architecture has been in development for nearly twenty years, we have no monolithic planner. The reasons are several-fold. One-Sim would have been both very deep and very broad – a challenging software development project taking years. During those years, each of the systems is evolving – simultaneously. Further, and probably most important, each of these systems is effectively in competition for acquisition funding by different branches of the military so sharing of technical details early to allow One-Sim development has many practical roadblocks.

5.2 Federated Planners

Today, MDA has embarked on a plan to implement federated planners exchanging schema-validated XML data. In the current CONOPS, a top-level planner can generate an initial plan that consists of defensive tasks. Each task is comprised of a threat, an asset and a defense system and is commonly referred to as task "triplets" – threat/asset/defense.

A drawing showing a tasking triplet is shown in Figure 5-2. In that example, there are multiple possible threat trajectories (shown as dashed lines) drawn to each critical asset (shown as a green circle). If you connect each threat-asset pair to each deployed defense system, then you develop tasking triplets. One such triplet (shown as yellow connection lines) is shown to the AEGIS ship.

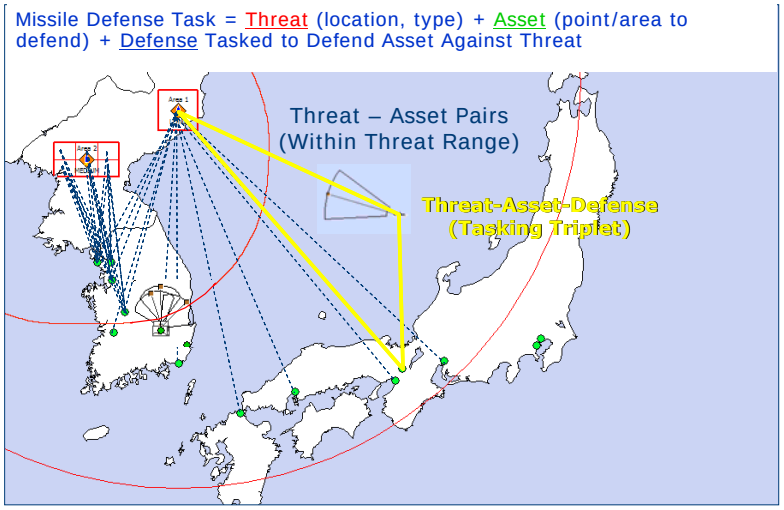


Figure 5-2: Using Threat-Asset- Defense Triplets to Analyze Performance

In the collaboration CONOPS, the full plan of proposed tasking triplets is sent to the tactical planner who is responsible for validating the tasks. This architecture is shown in Figure 5-3. Note the duplication of functions (e.g., three radar models).

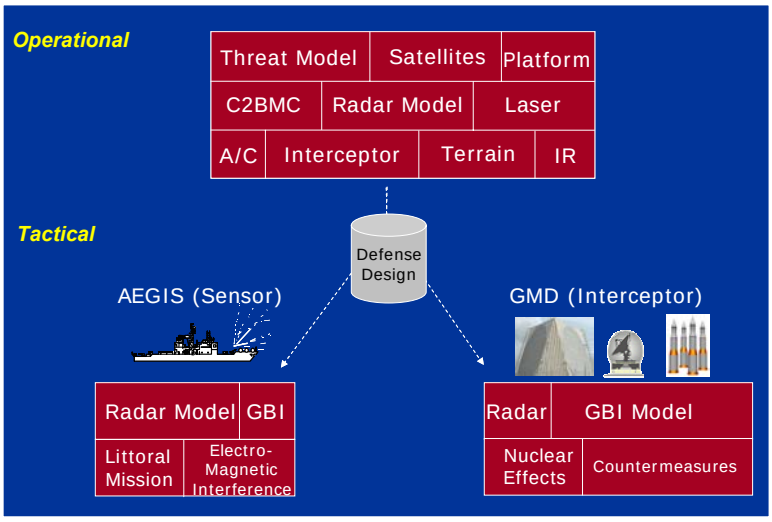


Figure 5-3: Example of Federated Planners in Missile Defense

The tactical planner receives the entire defense plan and may distribute the planning pieces down to each individual unit for validation. In the Army, their Air and Missile Defense Workstation (AMDWS) distributes the plan within their C2 structure to each PATRIOT unit involved. The units evaluate the tasks, by looking at the radar site, launcher locations, local weather conditions etc. AMDWS transmits the validation of the tasks or a suggested new location/orientation for the units.

The difficulty of this federated approach is that the tactical planners are asked to perform a high-fidelity assessment of their units' performance. If the unit uses external system data (e.g., a distributed sensor or weapon) to accomplish its mission, it needs to be able to model that interaction sufficiently for the validation. For example, for the Navy's AEGIS Destroyer to determine if its assigned location is adequate to support the Army's GBI, then AEGIS needs to model the performance of the GBI under varying AEGIS data conditions. The fidelity of the GBI model in the detailed AEGIS planner is often not sufficient to meet that need.

5.3 Net-Centric Planner with Distributed Physics-Based Services

The net-centric planner concept is basically a cross between the *One-Sim* concept and the federated planner. It is a deep and broad representation of the missile defense architecture with the components or functions of that model distributed. These components can run on different computers, operating systems and/or have been developed by different branches of the military. At a simple level, imagine a computer program that calls a radar subroutine or function. In the net-centric planner, the call is made to a web service that binds a missile defense radar application to the operational level planner to answer that specific question – how that radar performs a given task. The radar application responds to the question via web services much like a function or subroutine return.

An example of a net-centric planner architecture is shown in Figure 5-4. In this architecture, the operational level planner inputs the threat assessment, critical assets and

creates an initial plan or deployment of defenses. It calculates the architecture level performance using the web services developed with the tactical planners. (NOTE: if network connectivity is an issue, the operational level planner should retain default, local models in order to be able to plan on demand with graceful degradation).

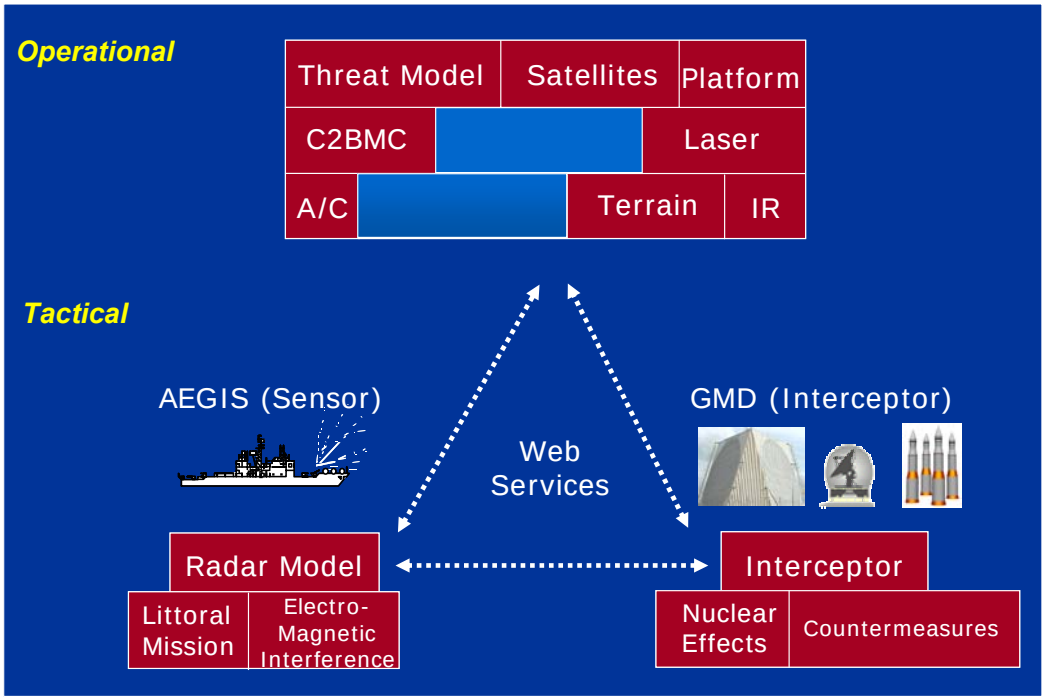


Figure 5-4: Example of a Net-Centric Planner

The tactical planners support the assessment of the architecture by answering physics-based questions for the operational planner (e.g., what is the flyout time for this engagement, can the interceptor support engagements at this altitude, what is the signal-to-noise ratio for a track of this type of threat at this aspect angle). The web services context diagram for this is shown in Figure 5-5. Each tactical planner publishes a list of the hosted services (i.e., questions that they can answer). A consumer (e.g., operational level planner) queries the registry to find a service that fulfills a requirement. For example, the AEGIS tactical planner finds a service published by the GBI tactical planner. The AEGIS radar model, then, resides only in the AEGIS tactical planner – not in the GBI tactical planner, as a duplicate function as was in the federated planner example.

Besides providing services to other components in the net-centric planner, the tactical planners also perform their own assessment – validation of the tasking triplets. To do that job, the tactical planners must rely on the external planners (via web services) that are involved in their systems interaction. Each tasking triplet is evaluated along with the evaluation of multi-mission aspects, water depth, terrain, electro-magnetic interference, etc. The tactical planner either validates the tasking triplet or can suggest a revised location/orientation that would be better suited for the defense performance overall.

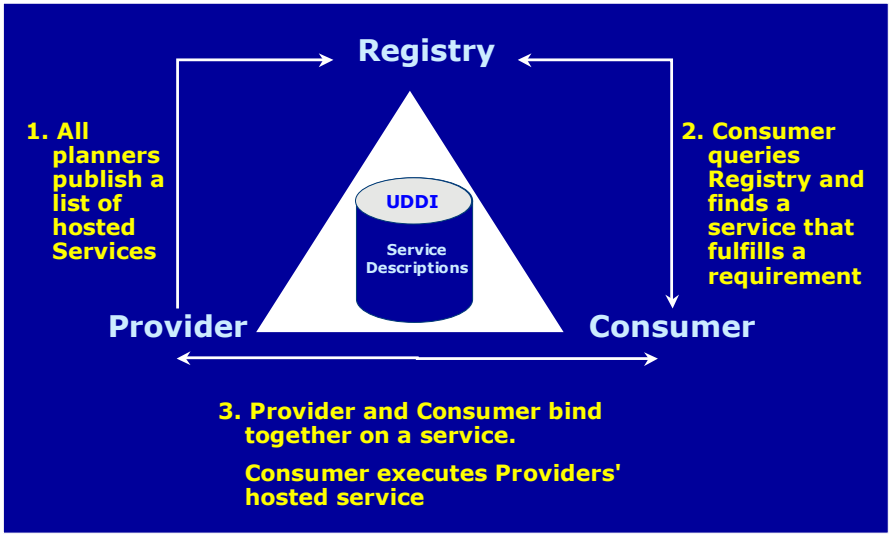


Figure 5-5: Context Diagram for Web Services

The tasking triplet is the central concept in the net-centric planner and even in the federated planner, although used in a less precise way for validation. If you consider all possible threat-asset-defense triplets in an AOR, you could construct a three-dimensional matrix. The resulting tasking triplet *results cube* is shown in Figure 5-6.

This cube can be created by the operational level planner. The operational level planner can make an assessment (although at a lower fidelity than the tactical planners) as to each defense's ability to detect or engage a threat going to a specific asset (e.g., one small cube in the matrix). If you look at the results for a single asset, you could think of that as the architecture probability of negation for that asset and plot that result on the map over the

asset. This is what was shown as a color code on our simple example in Figure 2-6. So, what is the role of the tactical planner a the results cube created at the operational level?

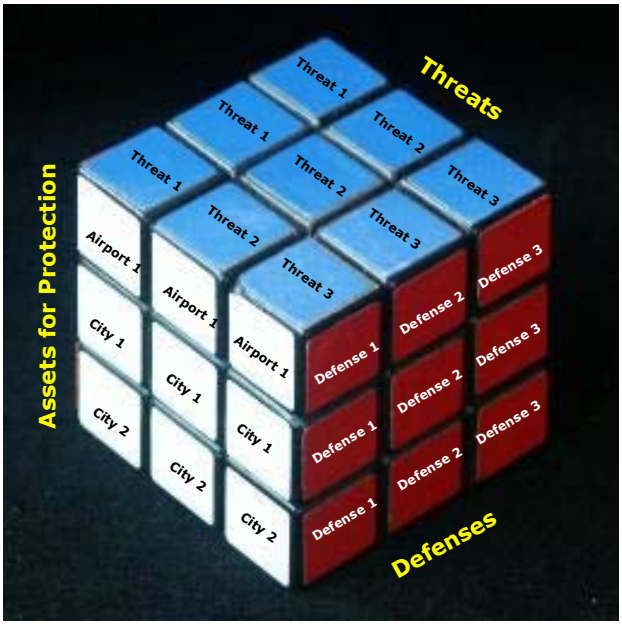


Figure 5-6: Using a "Results Cube" to Validate the Integrated Plan

The tactical planner evaluates the threat-asset pairs for its defense system (operating in the net-centric environment). This is evaluating one slice of the results cube and is shown in Figure 5-7 for a single defense system.

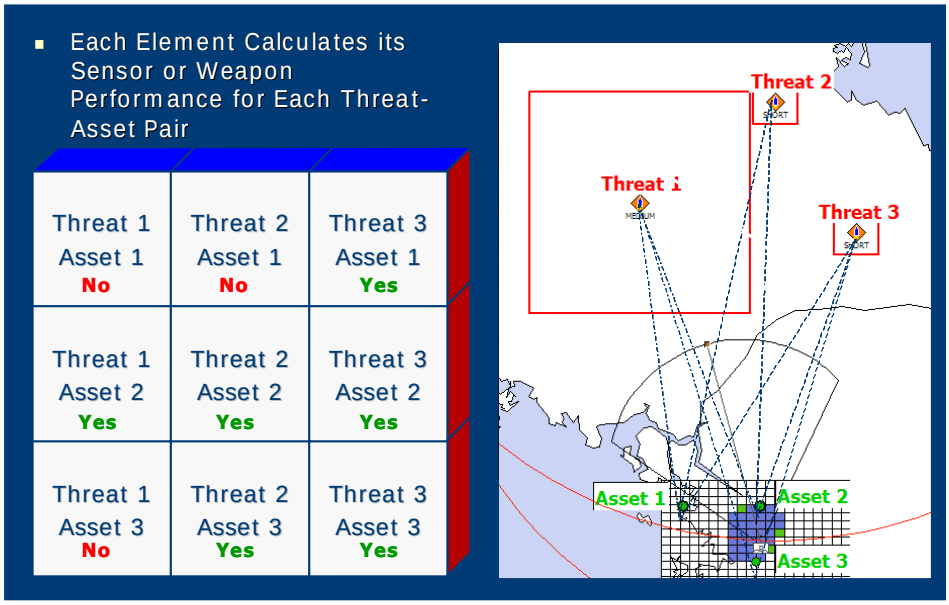


Figure 5-7: Analyzing Threat-Asset Pairs for Single Defense System

Each threat-asset pair is evaluated and can be reduced to a single yes/no response – although we advocate a technical measure of performance in addition. In the case of an interceptor system a result could be: "yes, I can engage threat 1 going to asset 2 at this probability of negation". In reality, there is a great deal of data behind the yes/no response. For a sensor, the tactical planner flys the threat missile, calculates the signal-to-noise ratio over time, places the threat target into track and reports on its track history. Examples of the data in each tasking triplet results cube for sensors and weapons is shown in Figure 5-8. On the left, the average earliest detection time is plotted on the map. For the location of an asset, a single value is known. The values of probability of negation for all threats to each asset is shown on the right.

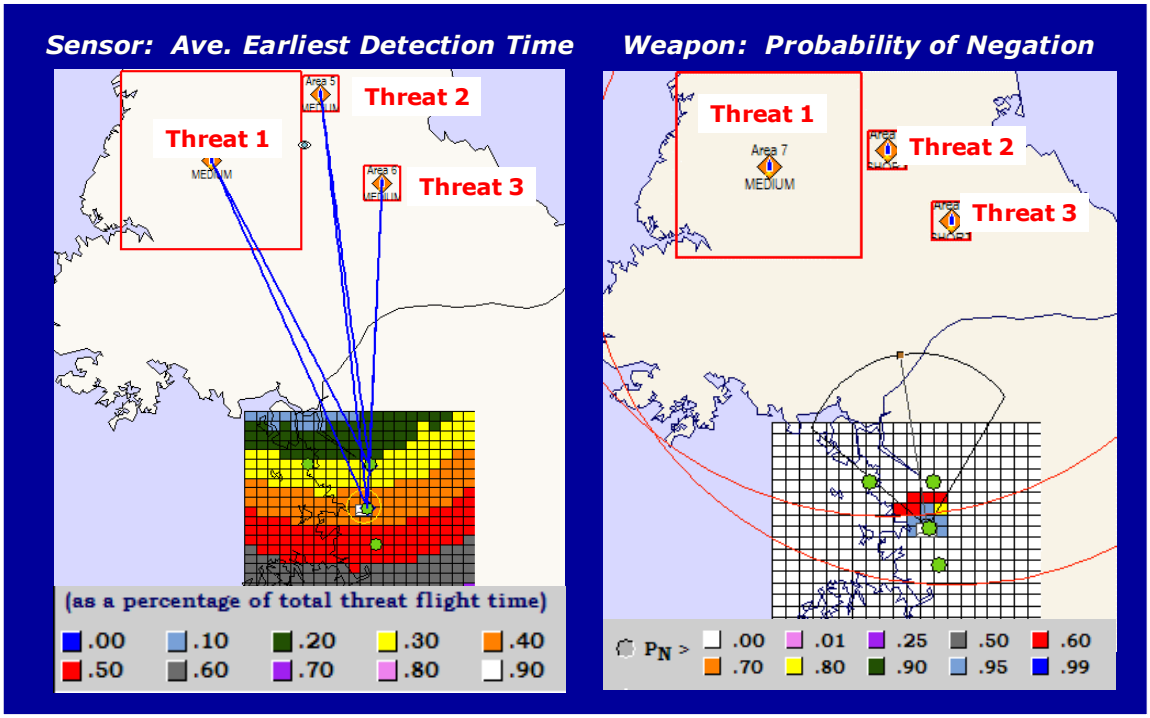


Figure 5-8: Example Measures of Performance for Sensors and Weapons

By using the results cube as the *glue* for the distributed planning, the warfighter can get a picture of the architecture performance. That picture can be for sensor or weapon measures of performance and, most importantly, it can be originally generated by the operational level planner and continued to be refined as the validation is complete by the

tactical planners. The user could even view the results cube and see what portions have been validated.

If a user of the tactical planner wants to revise his defense location or orientation, he can calculate two results cubes: one for the original situation and one for the proposed revision. Sending both cubes back to the operational level planner conveys the rationale behind the proposed change. If the change were accepted, another iteration of task validation by all elements in the architecture would automatically begin. Storing plan revisions and the status of cube validations allows the warfighter an ability to see the progression of the defense plan. This concept creates an approach to synchronizing the plan development through validation. The current plan is simultaneously being developed, evaluated, refined and validated – each iteration providing higher confidence to the warfighter. At any moment, the measures of performance indicating the results of the tasking triplet can be shown on the map – providing an intuitive assessment of the architecture capability. If the calculation considers each element on the map as a potential asset, then an entire region of the map can be evaluated in the same fashion, as was done for Figure 5-8.

6.0 Summary

The net-centric planner approach is the most viable concept for evaluating net-centric operations. It allows multiple legacy planners from each of the military services to come together over time. The traditional military service stovepipes can be integrated allowing each organization to have control over how its element is modeled and yet, let each planner become a component of the net-centric planner. As a tactical planner publishes his web service in the registry, the reliance on duplicate functions can be switched over. New elements or net-centric concepts can added from the beginning as a web service at either the operational or tactical levels allowing planning to occur quickly.

To accomplish net-centric planning, there are several steps that should be taken soon. These steps include:

- Development of an integrated missile defense approach to web services. This approach should determine, first, what physics-based questions could be answered and second, evaluate what the currently modeling approaches (e.g., common terrain, terminology and measures of performance).
- Determining CONOPS for Information Flow. If the network proves to be ubiquitous, then distributed functions should be satisfactory. If not, then certain functions should be duplicated at both the operational and tactical levels.
- Finalization of missile defense planning and intelligence XML schemas to accommodate Net-Centric planner needs. To accomplish this, the current schemas should be evaluated against the required breadth and depth (e.g., of the one-sim).

These next steps are not trivial but are certainly within the realm of today's technology and environment. A net-centric planner can be a fundamental capability in net-centric operations giving the warfighters a realistic assessment of what the defense architecture is capable of.

REFERENCES

1. Alberts, D.S, Garstka, J.J., and Stein, F.P. ***Network Centric Warfare 2nd Edition (Revised),*** Vienna, Va., CCRP Publication Series, 2002.

2. ***Defense Collaboration Tool Suite (DCTS),*** http://www.disa.mil/ca/buyguide/feature/dcts.html

3. Gardner, Tracy, ***An Introduction to Web Services***, IBM United Kingdom Laboratories, www.hursley.ibm.com

4. ***Simple Object Access Protocol,*** http://www.w3.org/TR/soap/ .

5. ***Universal Description, Discovery and Integration (UDDI),*** www.uddi.org

6. W3C, ***Web Services Framework for W3C Workshop on Web Services***, 11-12 April 2001, San Jose, CA USA

7. ***Web Services Description Language,*** http://www.w3.org/TR/wsdl .

2004 Command and Control Research and Technology Symposium
The Power of Information Age Concepts and Technologies

Challenges in Vertical Collaboration Among Warfighters for Missile Defense C2

Laura A.T. Lee, Ray C. Prouty, David J. Sepucha

SPARTA, Inc.
13400 Sabre Springs Parkway, Suite 220
San Diego, California 92128
(858) 668-3570

Challenge: Evolving Missile Defense Plans for Net-Centric Operations

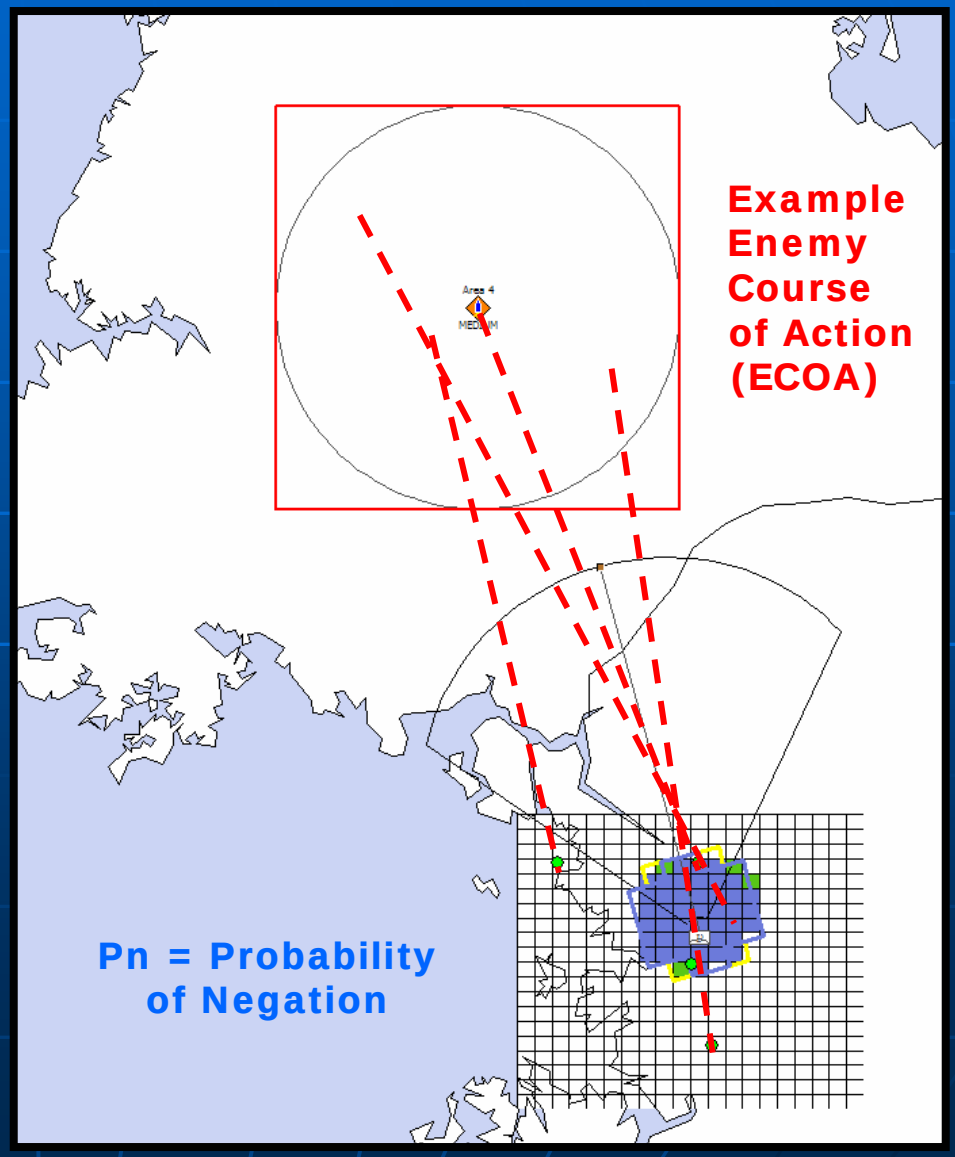
- In 2004, USSTRATCOM will Oversee the Deployment of the Initial Defensive Operation (IDO) for Missile Defense
  - Architecture Has Been in Development for Over Twenty Years
  - Comprised of Land, Air, Sea and Space Elements Developed by the Army, Navy, Air Force and the Marines
  - NCW Concepts Such As Networked Sensors Will Be Employed, Although Not Originally Envisioned
- The Corresponding Integrated Missile Defense Plan Must Consider the Complex, Distributed Sensors and Weapons From Around the Globe
  - The Plan Includes Tens of Systems Frequently Engaged in Multiple Missions for Different Commanders Against Multiple Threat Types
  - Individual System Planners Already Exist or Are in Development
  - Question is What the Role These Individual Planners Should Have in Integrated Plan for an NCW Architecture

Missile Defense 101

Enemy Missiles Have the Range to Be Launched in One Theater Area of Responsibility (AOR), Fly Over Another AOR and Impact in Yet Another AOR. With These Ranges, Missile Defense Has Become a Global Issue in Theater Conflicts.

Steps in Developing A Missile Defense Plan

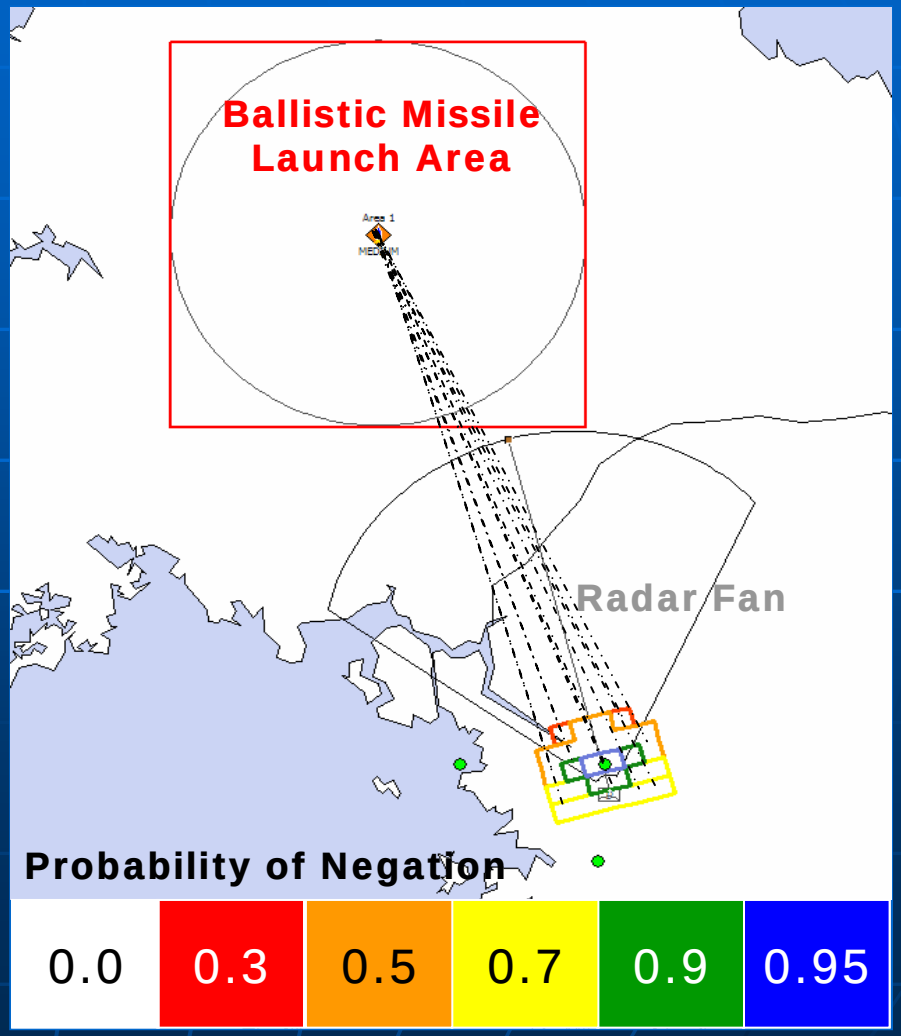
1. Gather Mission Guidance (current situation and plan objectives)
2. Analyze Defense Capability
   - Feasible Enemy Trajectories
   - Feasible Friendly Detections and Intercepts
3. Evaluate Enemy/ and Friendly Courses of Action
   - Most Likely Events
   - Includes Timing and Raid Size



Analyzing Complex Defense Capability

Increasing Complexity

- Single System, Single Threat (shown here)
- Single System, Multiple Threat Types, Single Mission (BMD)
- Single System, Single Threat, Multiple Chains of Command (AORs)
- Single System, Multiple Missions
- Multiple Systems, Interacting Systems, Single Threat
- Multiple Systems, Interacting Systems, Multiple Threats
- Multiple Systems, Multiple Threats, Multiple Chains of Command



Plan Development (Pre-Network Centric Warfare (NCW))

	Planning Focus	Products
Strategic	• Monitor Situational Awareness of Air Defense Plan	Theater Objectives & CINC's Intent / *OPLAN*
	Top Level Operational Planner	**Joint Force CDR** *Theater Campaign Plan*
Operational	• Develop A Prioritized Defended Asset List (Guidance) • Develop Intelligence Preparation of the Battlespace (IPB) • Evaluate Tactical Plans and Merge into An Operational Plan	**Joint Force Air Component Commander (JFACC)** *Air Campaign Plan* *Joint Air Operations Plan (MAAP, ACP)* Tasking/Coordinating (*TACOPDAT, ATO, ACO*) Situation Monitoring and Re-planning
	Detailed Tactical Planners	
Tactical	• Develop Plan Based on System Capabilities, Constraints for Optimal Locations	Missions (Plan, Execute & Assess)

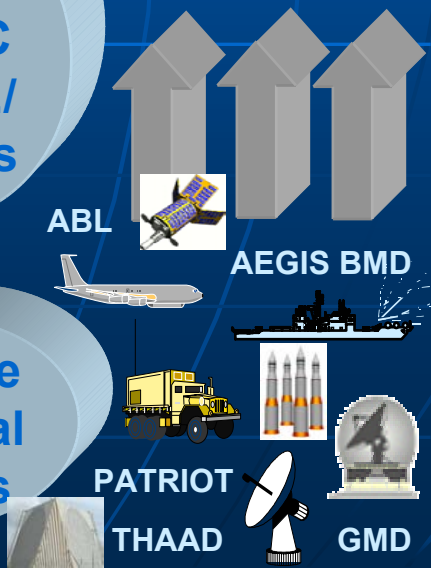
COCOM

JFC

JFACC /AADC Comp./ RADCs

Service Tactical Cmdrs

Tactical Plans

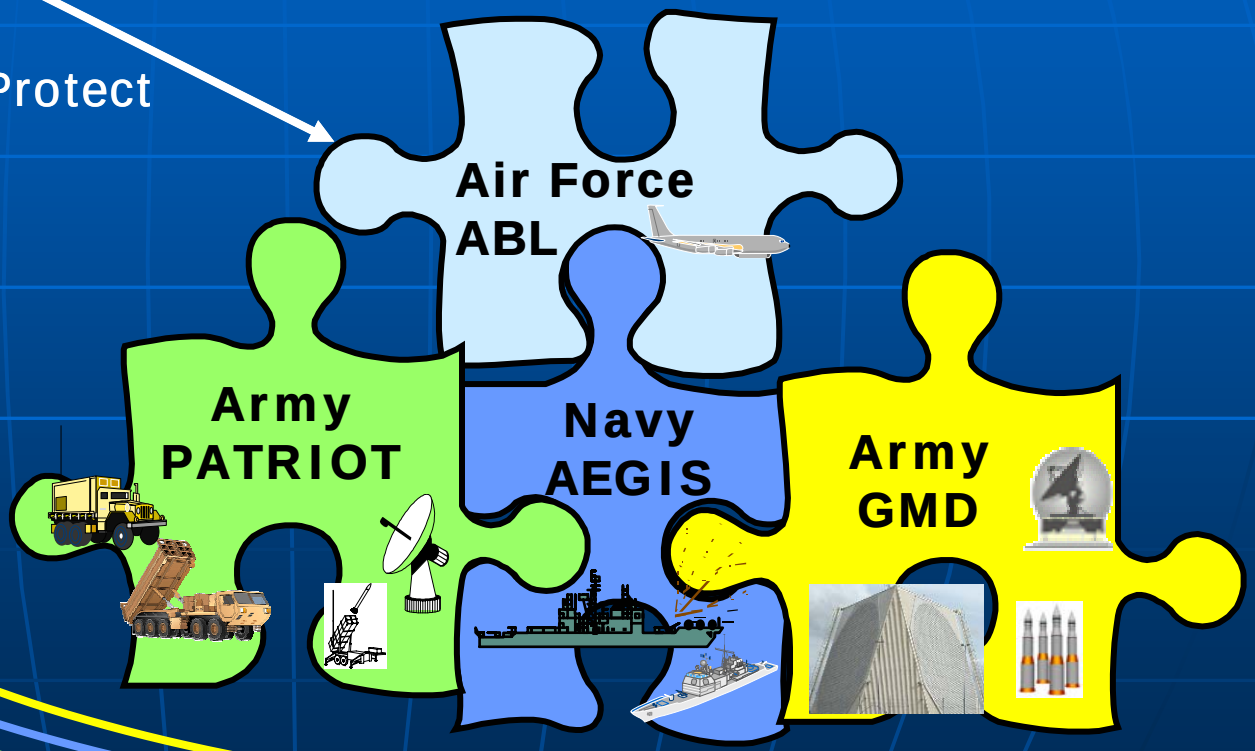


Building the Pre-NCW Operational Plan

Guidance

Threats,
Assets to Protect

"Integrated" Missile Defense Plan

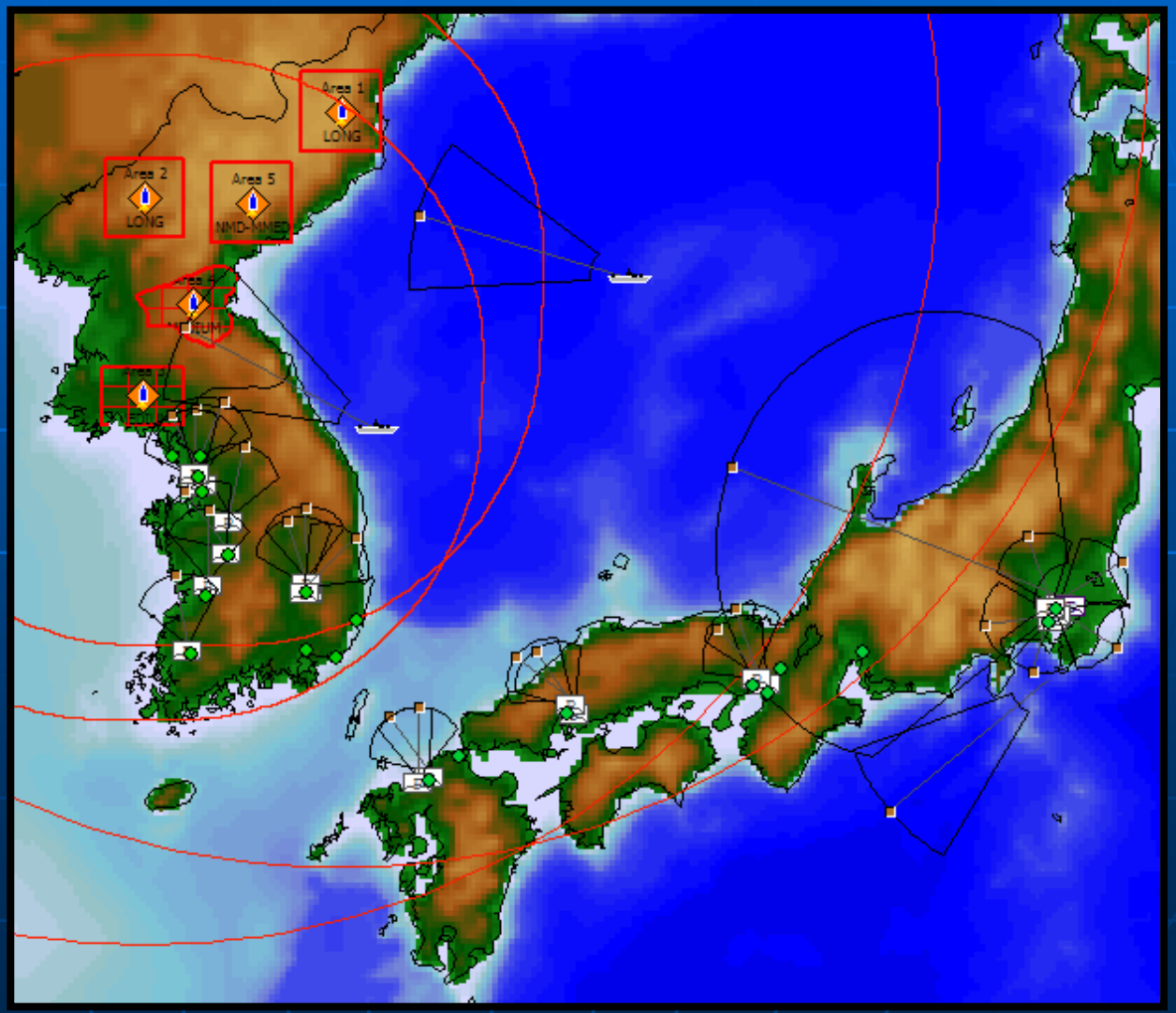


Not Really Integrated, But with Autonomous Systems, It Would Be Close

Plans

More Steps in Developing A Missile Defense Plan (Complexity) – A Tough Problem

- Multiple Systems With Intereactions (AEGIS SPY RADAR, AEGIS SM-3, PATRIOT RADAR, PATRIOT PAC-2/GEM/PAC-3, GBI, UEWR, COBRA DANE…), Multiple Threats (SCUD-B, SCUD-C, NO-DONG…), Multiple Chains of Command (USFK, USFJ, NORTHCOM)
- Multiple Missions (BMD, AAW…)
- Environment (Terrain, Water, Supportability, Electro-Magnetic Effects)



Planning Levels for Net-Centric Operations in Missile Defense

Strategic

- Monitor Situational Awareness of Air Defense Plan

Operational

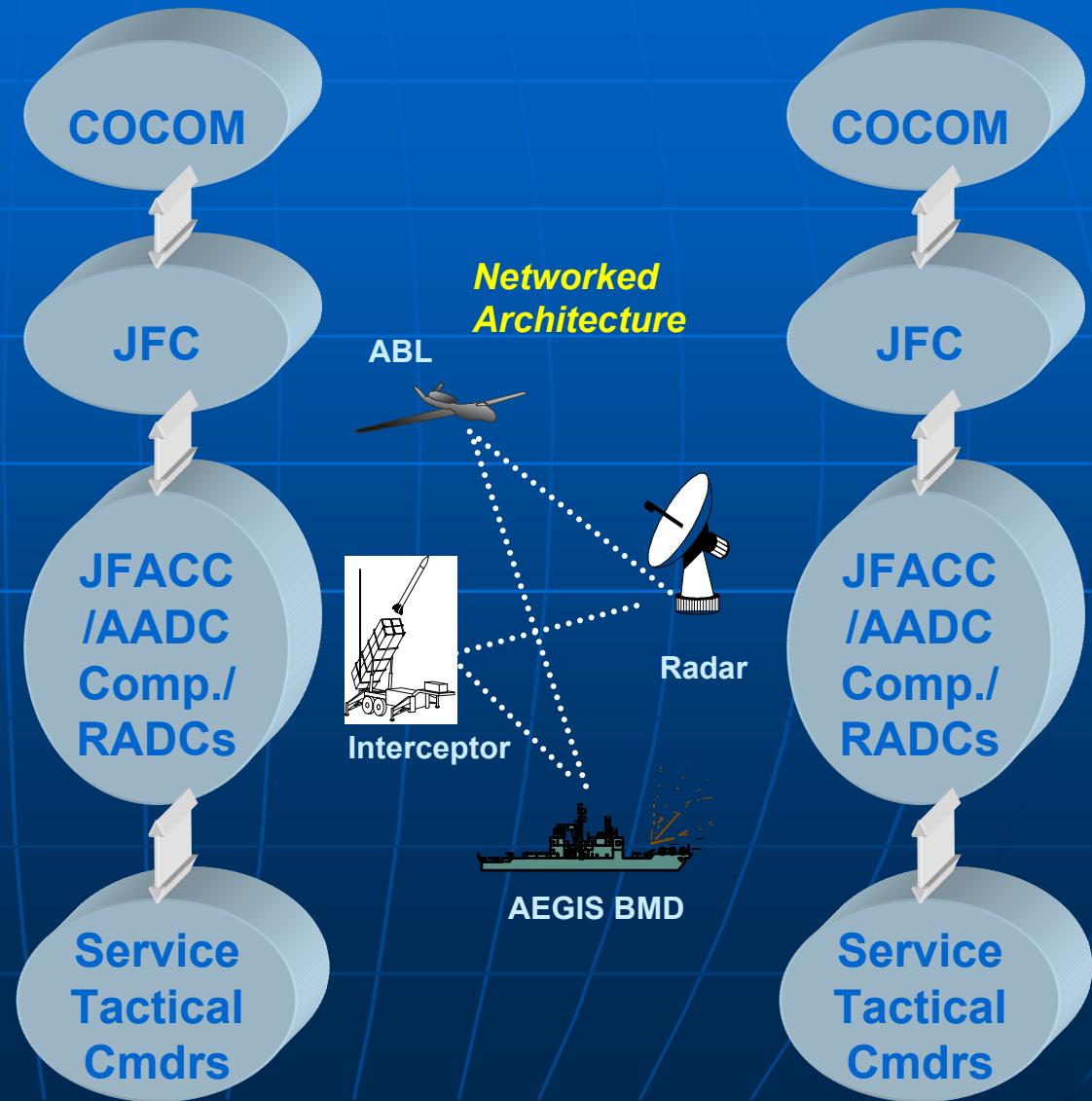
Operational Planner

- Develop Plan With Sufficient Detail to Recommend Options for Sensors/ Weapons
  - Includes C2 Such As Net-Centric Operations
- Evaluate Performance of Options to Illustrate Capabilities and Limitations to Decision Makers
  - Transmit to Lower Echelon Units for Refinement/Validation

Tactical

Tactical Planners

- Evaluate Tasking Based on Given Threat, Asset and Architecture
- Balance with Multi-Mission, Supportability, and Environmental Impacts



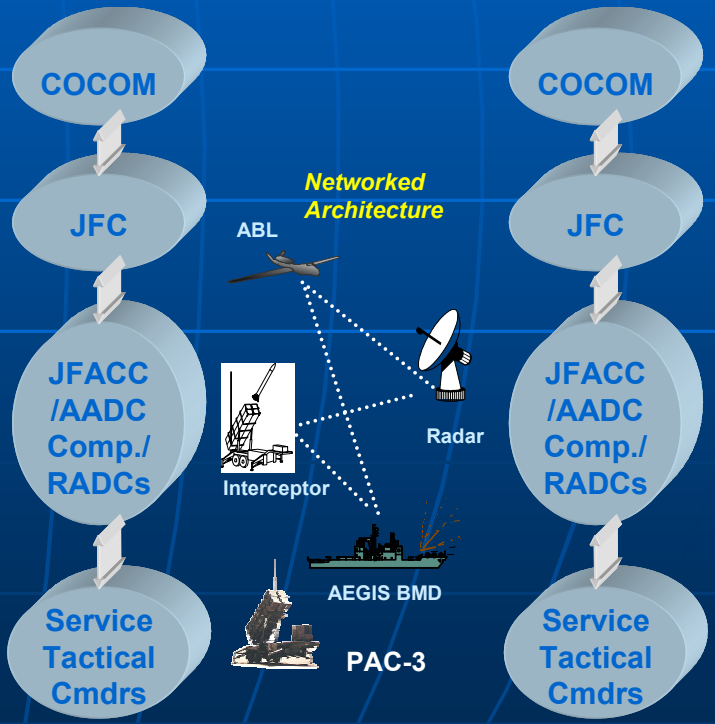
NCW: Now What?

1. SINGLE PLANNER. Build a Detailed Mission Planner (i.e., "One-Sim") for both Operational and Tactical Planning Levels

2. FEDERATED PLANNERS. Develop Medium Level Fidelity Planner for Operational Level and Collaborate with Detailed Tactical Planners

3. NET-CENTRIC PLANNER. Develop a Detailed Mission Planning Framework Comprised of Planning Services Performing Synchronized Development and Mission Validation

Options for Evolving Mission Planning for Net-Centric Operations



Option 1. Single Planner

Depth and Breadth

- Contains All Threats, Sensors, Weapon and C2BMC Models
  - Current Tactical Models Include Detailed Physics Algorithms (e.g., Detection, Clutter, Multi-path, Atmospheric Drag, Lethality, Weather)
- Considers Multi-Mission Aspects
  - Littoral Warfare
  - Air Defense (Aircraft, Cruise Missiles)
- Addresses Supportability, Reliability and Environmental Impacts
  - Road Networks, Water Depth & Channels, Terrain, Local Weather/Seas

Possible: **yes**

Likely: **No**

Why Not? Magnitude of the Problem (Breadth and Depth is Staggering), Engineering Details Are Evolving on all the Systems Simultaneously, Effort Crosses Service Boundaries with Acquisition Implications.

“One-Sim” Planner Example

Operational

Tactical

Threat Model	Satellites	Platform
C2BMC	Radar Model	Laser
A/C	Interceptor	Terrain	IR
Launchers	Anti-Air Warfare	EMI
Littoral Warfare	Supportability

...

Option 2. Federated Planners

- Essentially, the Current Situation
- Top Level Operational Planner Evaluates Threats, Assets and System Elements for Defense Capability
  - Creates Tasking (threat + asset + defense triplets)
  - Evaluates Architecture Performance
  - Requests Refinement by Tactical Level Planners
    - Tactical Planner Submits Task Validation, Suggests New Location/Orientation and Additional Assets for Protection
  - Submits Final Plan
- Registered XML Schema for Threat Input and Missile Defense Design (Plan) Assists In Collaboration
- Refinement by Tactical or Service Planners Can Be Difficult, Unless Each Planner Can Model the Other Sensors or Weapons They Interact With (e.g., Navy AEGIS Models Army Ground-Based Interceptor)

Federated Planner Example

Operational

Threat Model	Satellites	Platform
C2BMC	Radar Model	Laser
A/C	Interceptor	Terrain	IR

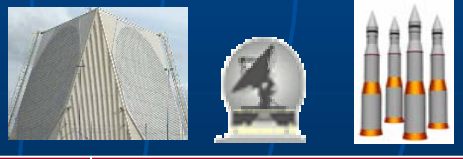
Tactical

Defense Design

AEGIS (Sensor)

Radar Model	GBI
Littoral Mission	Electro-Magnetic Interference

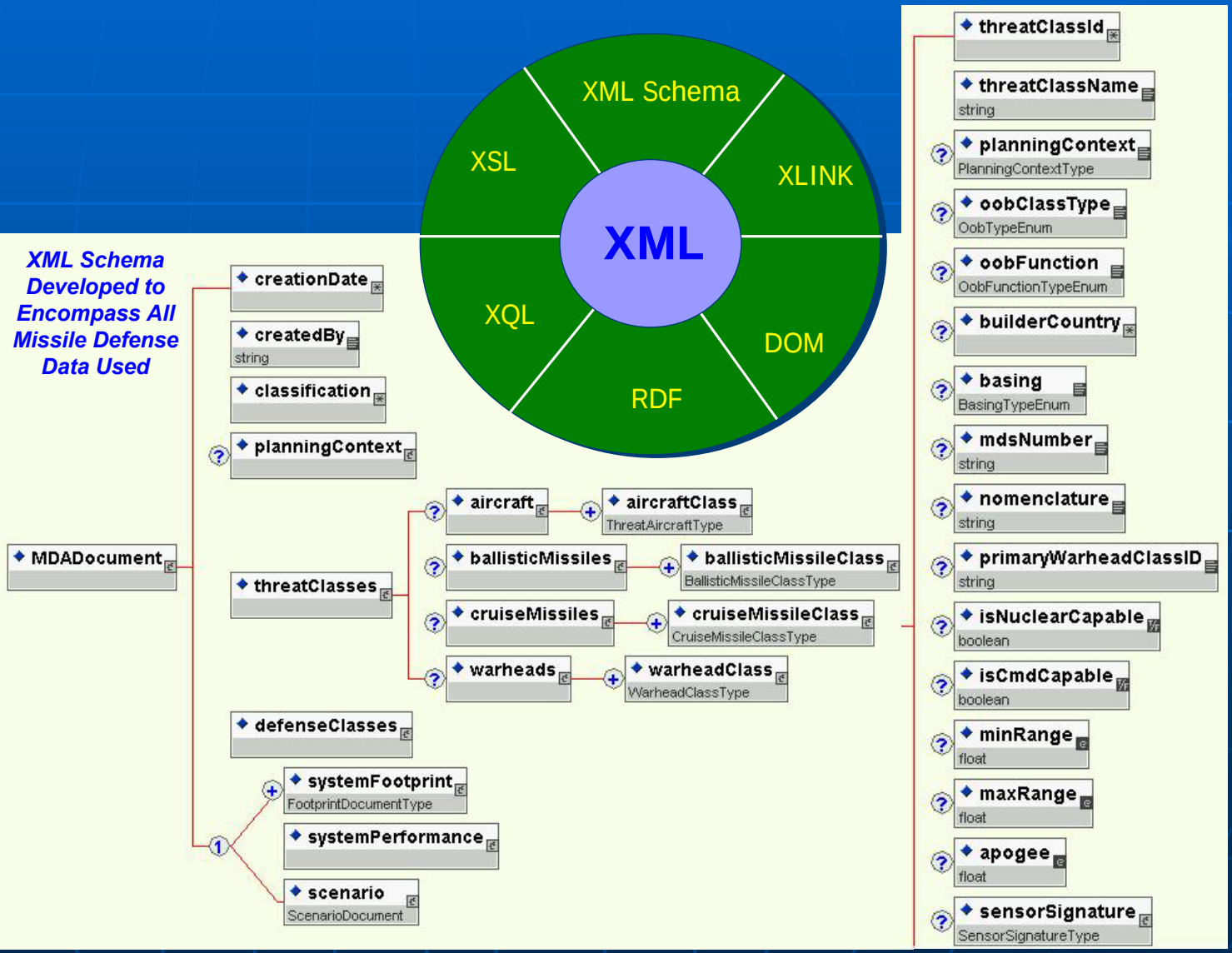
GMD (Interceptor)



Radar	GBI Model
Nuclear Effects	Countermeasures

Technology Advances Supporting the Collaboration Among Planners

- eXtensible Markup Language (**XML**)
  - Missile Defense Agency (MDA) Developed an XML Schema for the Missile Defense Planning Data
  - Defense Intelligence Agency (DIA) Developed an XML Schema for Ballistic Missile Threat Data
- MDA's Operational Level Planner Employed the **Java Messaging Services** (JMS) to Exchange Plans
- MDA and the Army Are Developing A **Web Service** Interface To Validate Tasks Among Their Planners



Web Service Standards Used To Support Net-Centric Planning

- eXtensible Markup Language (XML)/ XML Schema Definition (XSD)
  - Syntax for Messages and Data Types
- Hyper Text Transfer Protocol (HTTP)/ Simple Object Access Protocol (SOAP)
  - Transport and Syntax for Synchronous/ Asynchronous Messaging
- Web Services Description Language (WSDL)
  - XML Format for Describing Network Services
- Universal Description, Discovery and Integration (UDDI)
  - Registry model supporting 'publish, find, bind, execute'
- Web Services: WS-Security, WS-Transaction, WS-Coordination
  - Syntax for reliable messaging, encrypted payloads

Option 3. Net-Centric Planner

- Operational Level Architecture Planner Evaluates Threats, Assets and System Elements for Defense Capability
  - Creates Tasking (threat, asset, defense triplets)
  - Evaluates Architecture Performance Using Web Services for Element Capability
  - Publishes Initial Plan

- Each System Element (sensor or weapon) Subscribes to Missile Defense Plans
  - Evaluates Tasking
    - Identifies Any Issues with their Element Locations
      - Multi-Mission Impacts, Water Depth, Terrain, Electro-Magnetic Interference
    - Calculates Element Performance for Each Threat-Asset Pair
      - Sensor Elements Produce Detection/Track History or Signal-to-Noise Ration (SNR) plots
      - Weapon Elements Produce Probability of Negation Contours for Their Weapon using the Sensor Network
    - Validates Tasking for Original Location/Orientation or Suggests Revised Location/Orientation Showing Original and Revised Validation Matrices for Approval (which starts cycle of iteration)

What Happens When One Element Suggests a Revised Location/Orientation….The Plan Development Must Be Iterative.

Net-Centric Planner Example

Operational

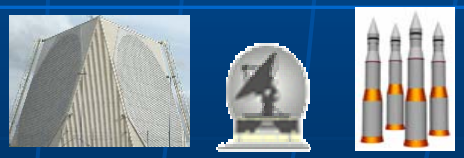
Threat Model	Satellites	Platform
C2BMC		Laser
A/C		Terrain / IR

Tactical

AEGIS (Sensor)

Web Services

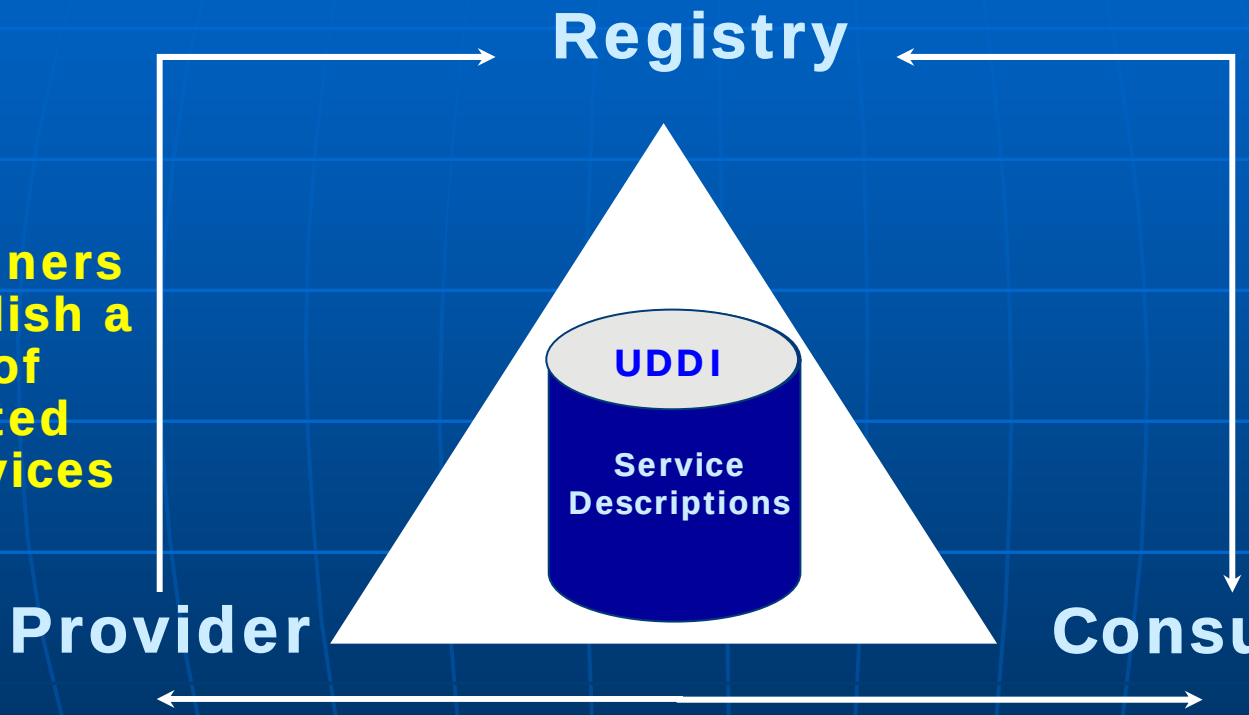
GMD (Interceptor)



Radar Model	
Littoral Mission	Electro-Magnetic Interference

Interceptor	
Nuclear Effects	Countermeasures

Web Services Context Diagram



1. All planners publish a list of hosted Services

2. Consumer queries Registry and finds a service that fulfills a requirement

3. Provider and Consumer bind together on a service.

   Consumer executes Providers' hosted service

Net-Centric Planner Example

AEGIS (Sensor)

Planner #1
Radar Model

Web Services

Planner #2
Interceptor

GMD (Interceptor)

Planner #1

Planner #2

Planner #3

Planner #4

Service Registry

AEGIS Radar	GBI Int
Service Descriptions	
UEWR Radar	AEGIS Int

Net Centric Planner

Service Deconfliction

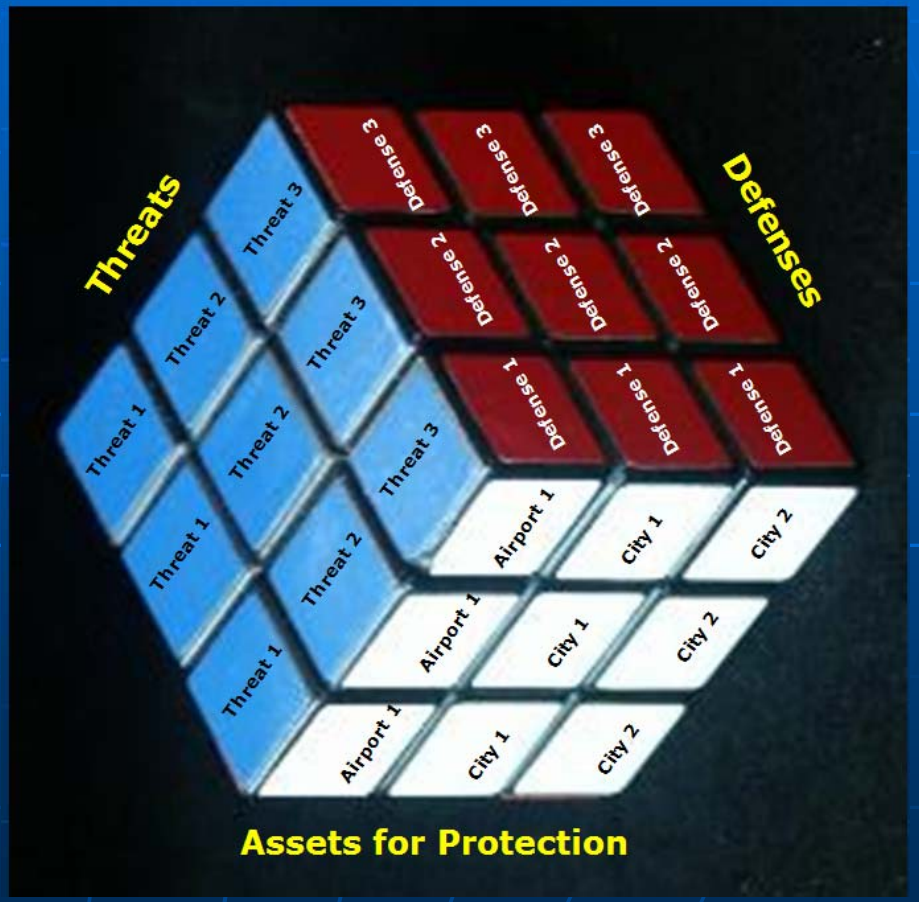
Integrated Planner

Threat Model	Satellites	Platform
C2BMC	Radar Model	Laser
A/C	Interceptor	Terrain	IR
Launchers	Anti-Air Warfare	EMI
Littoral Warfare	Supportability	

Integrated Plan

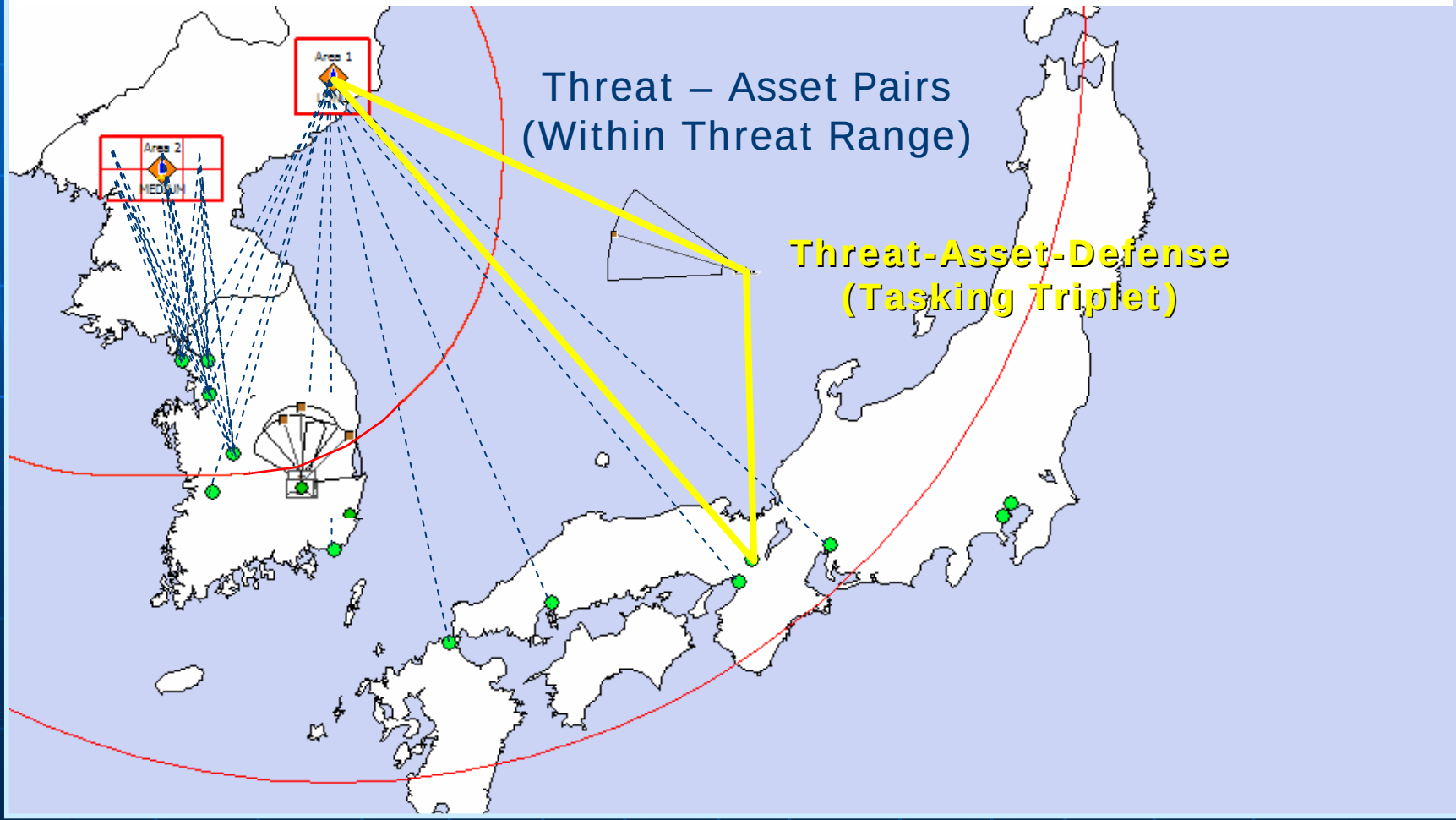
The Plan "Glue": A Results Cube

- Operational Planner Constructs a Threat – Asset-Defense (Tasking) Results Cube
  - Task (Cube) Can Contain Original Performance, Validation Attribute and Validated Performance
    - Tactical Planners Can Validate Each Task (Initial Plan with Improving Confidence)
- Results Can Be Translated into Probability of Negation Contours – Color Coded for Intuitive Reading



Tasking Triplets

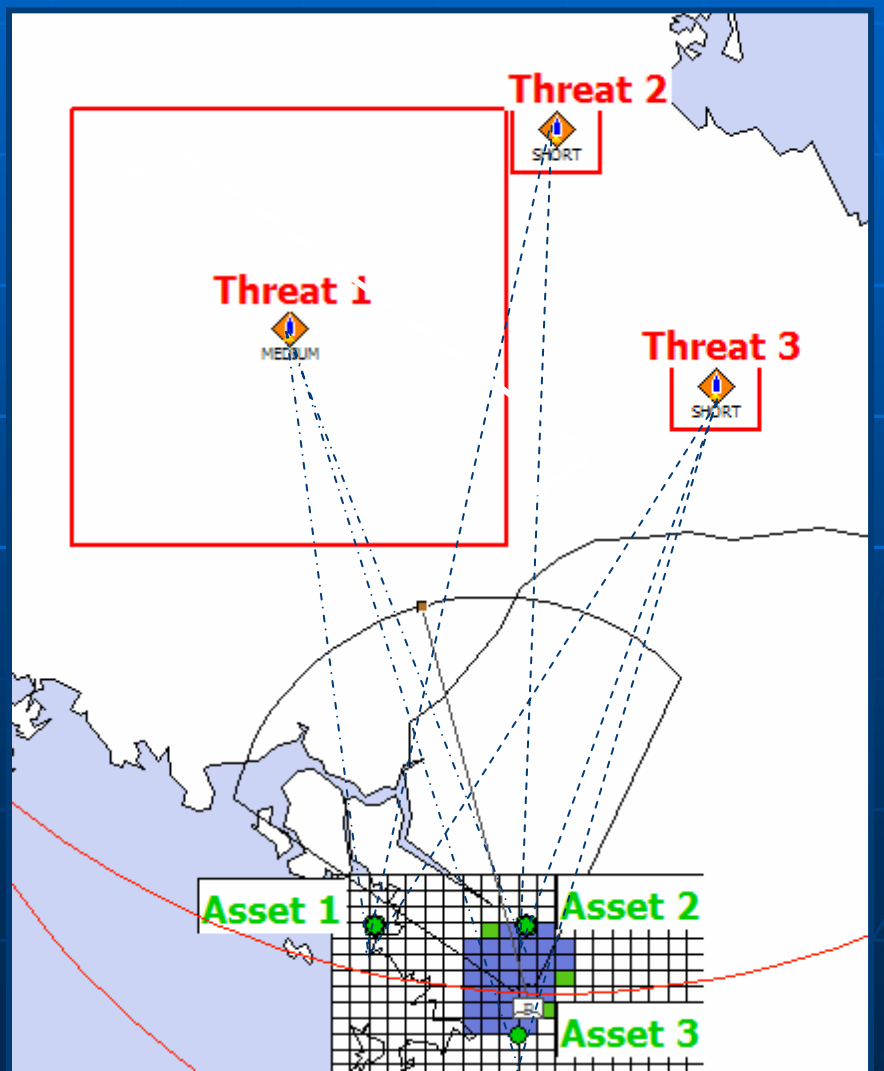
Missile Defense Task = Threat (location, type) + Asset (point/area to defend) + Defense Tasked to Defend Asset Against Threat



Tasking Details for One Defense Element

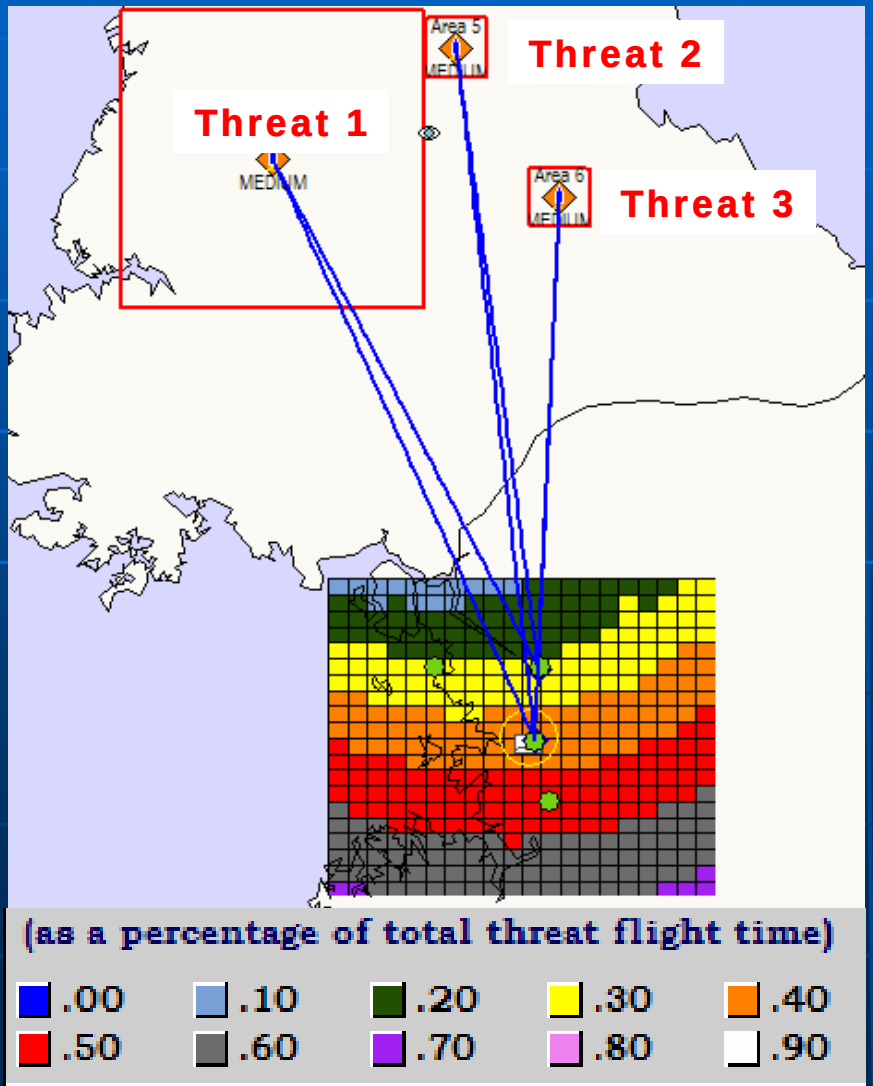
- Each Element Calculates its Sensor or Weapon Performance for Each Threat-Asset Pair

Threat 1 Asset 1 **No**	Threat 2 Asset 1 **No**	Threat 3 Asset 1 **Yes**
Threat 1 Asset 2 **Yes**	Threat 2 Asset 2 **Yes**	Threat 3 Asset 2 **Yes**
Threat 1 Asset 3 **No**	Threat 2 Asset 3 **Yes**	Threat 3 Asset 3 **Yes**

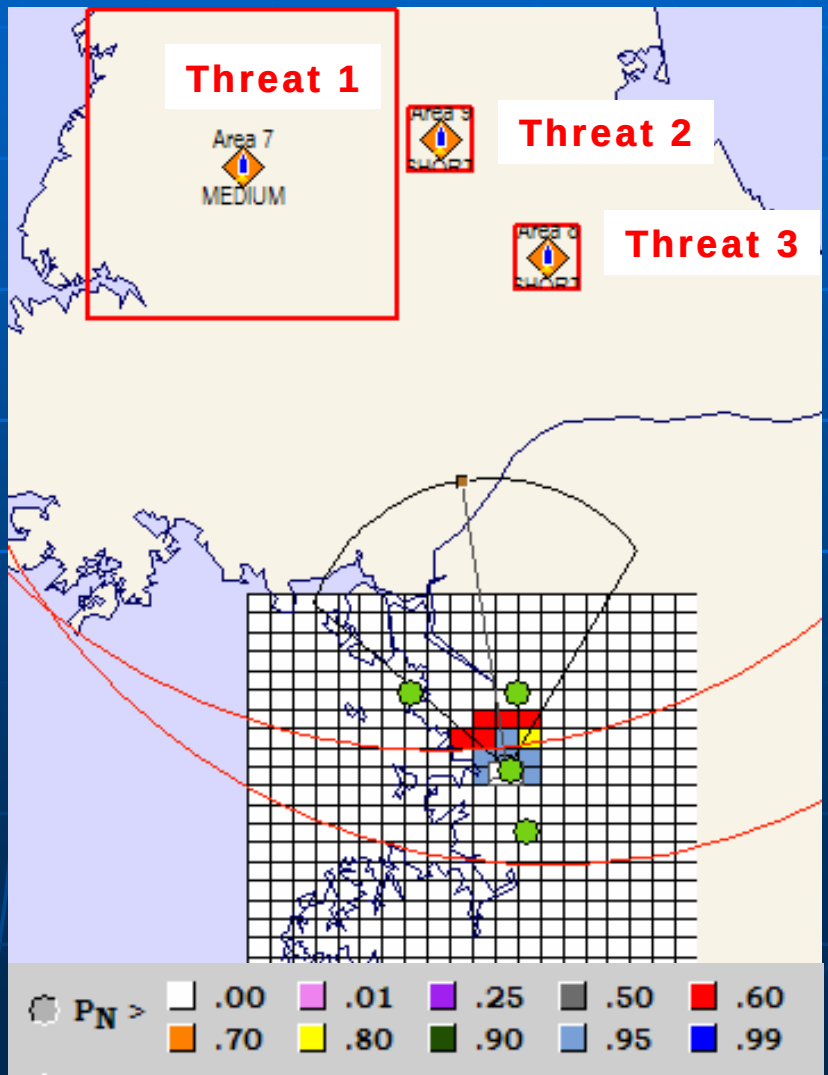


Example Results for Sensors and Weapons

Sensor: Ave. Earliest Detection Time



Weapon: Probability of Negation



Next Steps for Net-Centric Planning

- Develop Web Services Approach Across Missile Defense Planners
  - Determine What Physics-Based Questions Can Be Provided?
  - Evaluate Modeling Approaches Across Planners (e.g., common terrain, terminology, measures of performance)
- Determine CONOPS for Information Flow
  - Is Network Ubiquitous or Should Operational Level Planner Retain Duplicate Models to Gracefully Degrade?
- Finalize Missile Defense Planning and Intelligence XML Schemas to Accommodate Net-Centric Planner Needs
  - Evaluate Current XML Schemas Against Required Breadth and Depth

Summary

- Missile Defense Planning Incorporating NCW Concepts Is Complex
- Several Options Exist to Develop and Validate the Plan
  - Single “One-Sim” Planner
  - Federated Planner
  - Net-Centric Planner
- Choosing a Net-Centric Planner Solution Provides the Best Path To Evolving the Current Missile Defense Planning Process